Jody Bauer, VP ITS & CIO

The new buzz in technology, cloud computing, requires us to review our service offerings in a new light -- especially as we move into an era of mobile and open access computing.

As we start to explore the cloud as a fit for the College, many issues will present themselves to us. Most of these will be answered by our risk tolerance level. Among these are: (1) should we move some or all our data and applications into the cloud, (2) what are the security risks we are ready and willing to accept to move to the cloud, (3) are we willing to lose control over service availability by moving into an environment that is controlled by others? These and many other questions will be discussed.

We may view the cloud as a cost savings measure that will give the institution agility in the technical environment. This and other factors have initiated the College's move to some cloud services. These services are hosted off-site either at a cost or free due to our academic affiliation. We provide student e-mail services via Google Apps, the employment application process is supported by PeopleAdmin for Human Resources, credit card processing is done off-site with a PCI compliant vendor and student assessment testing is accomplished using the web via COMPASS. Many academic departments are engaged in the Cloud by utilizing testing and text book supplements. The list of services moving to the Cloud continues to grow daily.

Even some of our ERP application services might be moving into a secure cloud environment. Our vendor, Sungard Higher Education (SunGard HE), is already moving in that direction. Their needs analysis calculation for financial aid is available in a subscription-based solution which hosts the needs calculation algorithm while data remains within the College database.

Statistics show that over 80% of large organizations (1000+ employees) have at least one cloud service and more often they have six. Collaboration services lead these deployments, with hosted email, anti- virus/spam filters and web conferencing the most common applications being deployed into the cloud by large enterprises.[i]

If we are already in the cloud, what are the decisions around moving deeper into a hosted environment? What are the true barriers to moving to the cloud for the College?

First let us identify some of the terminology we will be using when discussing the cloud.

Definitions

First, what is the cloud? The cloud is short for cloud computing, which, at its simplest, is the ability to use the Internet to access technology-based services. The keys are that the user accesses resources through an Internet browser or mobile device and the physical location of the resources is transparent to the end user.

A more formal definition from the National Institute of Standards and Technology (NIST) is a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[ii].

This definition incorporates several of the key characteristics that make a service a cloud service. **On-demand** implies that the user can increase capabilities without intervention with the service provider. **Network access** implies the services are available through standard platforms that are readily available on existing platforms (desktop or mobile devices). **Shared pool** means that multiple users of the cloud service provider can benefit from the collective capacity of the service provider hardware and/or software as necessary. There is no control over the actual resources being used by a user. This is often referred to as a multitenant model. **Rapid provisioning** implies that capabilities can be dynamically added and removed as necessary to increase scale or remove when no longer necessary. The only other key characteristic of cloud computing defined by NIST is that the service is **measured**. This implies that the service provider meters and monitors activity in the way that a water or electricity utility provider might need to – to respond by charging the consumer appropriately and adding hardware and/or software appropriately.

The concept of cloud computing fills a perpetual need of IT: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends ITs existing capabilities.

Second, what delivery options are available for cloud services? There are currently three service models for cloud computing: Infrastructure as a Service (**IaaS**), Platform as a Service (**PaaS**) and Software as a Service (**SaaS**).

IaaS providers offer hardware infrastructure over the Internet. There are several different variations of IaaS provider services, but, generally, these services can provide servers, storage, processing power, test and development environments, et cetera. IaaS providers

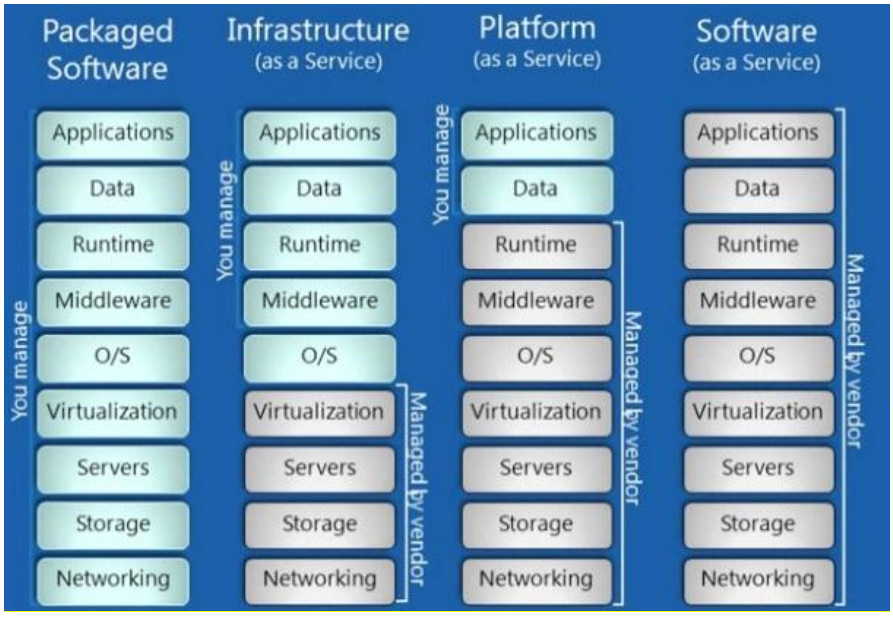
offer consumers virtual server resources and the supporting infrastructure, managed by the provider, on which the consumer installs and maintains operating systems, applications and/or data. The provider manages components related to the server: physical security, networking, hardware such as hard drives, backup and operating system virtualization. The consumer must manage the operating system and applications. Examples include AWS from Amazon and Hyperion from Secure-24.

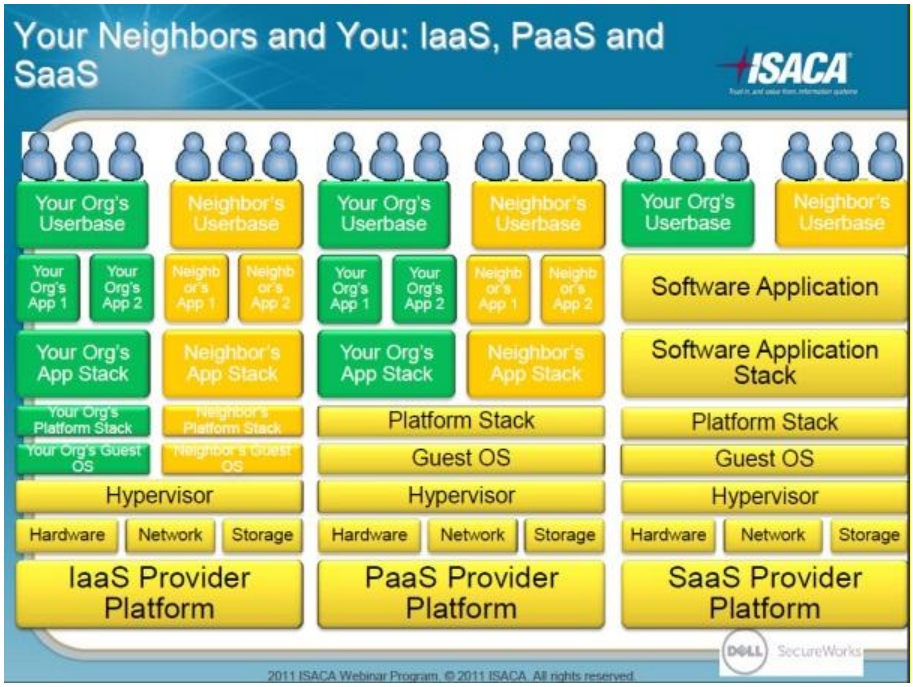
PaaS providers extend what IaaS providers offer by adding operating system and application management. PaaS provides a hosted application or framework with a set of software tools to facilitate application development or team collaboration. An example of these service offerings are Microsoft Azure with VM, force[dot]com and Amazon's EC2. We should note here that the economies of scale will always be with Public Cloud PaaS providers.

SaaS providers extend what PaaS providers offer by adding application management. Software and the associated data are hosted by the SaaS provider. For example, Gmail is a type of a SaaS provider because you don't have to manage any e-mail software or data as a Gmail user. All of that is accomplished by the provider, which is Google. SunGard HE's provisioning of a component of the Banner Financial Aid system for needs analysis calculations is another example.

Figure 1 provides a visual comparison of the three service models as compared to owning and managing software. The figure shows the components involved and who is responsible for the management in a standard (i.e., packaged software) environment as compared to a cloud environment.

Figure 1 - Cloud Service Model Comparison





The architecture that SaaS providers deploy varies; however, the variations tend to be one along the lines of multitenancy. **"Multitenancy"** refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants). Multitenancy is contrasted with a multi-instance architecture where separate software instances (or hardware systems) are set up for different client organizations. With a multitenant architecture, a software application is designed to virtually partition its data and configuration, and each client organization works with a customized virtual application instance."[iii] The most pure form of multitenancy has all customers running on the same version of software and data structure[iv].

Third, what options exist for cloud service deployment? There are four: public cloud, private cloud, community cloud and hybrid cloud.

Public clouds are the most common cloud deployment method. In this deployment, all physical resources are owned by the service provider available to clients through the Internet[v]. Examples include offerings by Amazon (Elastic Compute Cloud), Google Apps and Windows Azure.

Private clouds are intended only for a specific organization. It can be managed by the organization at the organization premises or by a service provider at the service provider.

Community clouds are an infrastructure shared by many organizations with a common community goal. These are managed by organizations or a third-party and may exist on premise or off premise. An example could be the formation of a community cloud to service the 14 Pennsylvania Community Colleges through the Commission and supported by the KIMBER Pennsylvania Research and Education Network (PennRen) consortium.

Hybrid clouds are an infrastructure that is comprised of two or more clouds (i.e., a public and a private cloud) that are separately managed but work together to achieve an organization's goals. An example might be to use a public cloud to develop and test applications before releasing them on internal networks[vi].

Business Drivers

When an organization considers outsourcing an environment or a business process, it is important to understand both the benefits and the risks presented by such a move. The benefits of moving to the cloud include the following:

- Ability to better align IT with business. Effort can be applied to supporting the functions that are essential to delivering core business functions. For higher education, this might include such functions as instruction and education, developing graduates, increasing graduation rates, et cetera. The IT resources that would have been dedicated to support and maintenance of the outsourced environment can become available for other tasks more closely aligned with the core business function.
- Scalability and flexibility. A benefit of the cloud is its ability to offer adopters the capacity to gain system resources as needed (i.e., scalability) and to do so quickly and for the time periods it is needed the most (i.e., flexibility). The College has many of its most critical servers on a multi-year lease schedule, which enables us to migrate to more robust technology offerings on a regular, fixed basis. By doing this, we have the ability to increase throughput on servers and evaluate efficiencies, on a regular and fixed basis. However, this does not come without significant planning, testing, documentation and communication efforts by ITS. By moving to cloud offerings, we might be able to shorten this window from multiple years to potentially as little as a matter of minutes.
- Immediacy and efficiency. The cloud allows for dynamic allocation of additional resources as needed – thus having an aspect of immediate response to demand. Another way in immediacy is a benefit is in startup or implementation time. Cloud service providers are constantly monitoring and evaluating infrastructure needs and responding by adding additional resources as necessary. Cloud service providers also have professionals who are experienced with a range of technologies the providers offer and support. This means that the providers can implement new environments for clients within a shorter window of time than the client organization. We could take advantage of a reduced implementation time and learning curve for our own staff.
- Low overhead. Depending upon the type of cloud offering, the overhead cost of moving to the cloud could easily be lower than the cost to implement in-house. Annual maintenance costs might be lower, the overall cost could be lower with a pay-as-you-go model and there could be less unscheduled break/fix costs.

Critical Issues

With all of these benefits, one might ask why all of our environments and processes are not yet in the cloud. To fully evaluate this, it is critical to understand the issues and risks presented with moving to the cloud. They include:

1. Security. The number one risk presented by the cloud is security. At a minimum, any cloud service provider considered should be compliant with security-oriented laws and auditing programs, including Safe Harbor, ISO 27001, and SAS70 Type II. We are still responsible for the integrity and security of our data, even if it physically resides with the cloud service provider. Security can be thought of in a variety of ways[vii], as follows:
    a. Privileged user access. Privileged user accounts are the most powerful accounts. These types of accounts include system administrator access to operating systems, database administrator (DBA) access to databases, generic system accounts that are created with installations, et cetera. Moving our data to a cloud service provider means that we bypass the in-house controls that we have implemented for access to these privileged users. It is critical to have conversations with the cloud service provider to understand what methods are employed to control privileged user access.
    b. Physical security. We transfer control of who has physical access to the hardware supporting our application and data to the cloud service provider when purchasing cloud services. With a data center maintained at main campus, we can fully restrict staff that can enter and access the data center.
    c. Network and perimeter security. We also transfer control of network security to the cloud service provider when purchasing cloud services. Thorough disclosure on the part of the cloud service provider as to how they secure the servers on which applications and data reside is critical to understanding how much risk exists in this area of security.
    d. Data segregation. Many cloud service provider employ the multi-tenancy model, which places many clients on the same hardware and potentially even within the same software installations, depending upon the service offering. We rely on the cloud service provider to indicate whether our data (and backups and logs) are distinct from other clients' data (and backups and logs).
    e. Financial security of cloud service provider. *What happens to your data when the Cloud provider is not fiscally viable any longer?* Cloud services have existed for many years. As with all technology, changes occur and we all remember the dot com boom-bust era. A consideration within the planning of any Cloud move is the ownership of the College's data and how that data will be maintained if the provider has a catastrophic event or must close their provider service.
2. Legal issues
    a. Regulatory compliance. We retain some very key data about our students, employees and constituents, among others. In some cases, this data is governed by federal or state laws, such as the Family Educational Rights

and Privacy Act (FERPA - which pertains to the release of and access to educational records). In other cases, the data is highly personal and sensitive and meant for a restricted set of staff, such as information pertaining to financial aid, salary and benefits, donor giving history, disabilities, et cetera.

   b. Data location. For certain industries or certain data, there are restrictions on whether data can be stored in certain countries. This would include data, any intermediate data storage locations and data backup locations[viii].
   c. E-discovery. The need to maintain data in its original format is a necessity in this century. E-discovery requests from legal counsel require that immediate actions be taken to recovery and store data and email in its original format until released. Any Cloud provider must provide this access through archiving of data and email. Such provisions come with a cost per user and should be part of the calculated cost of any Cloud move. In addition to providing this archive service, College network administrators must have access to the data without encountering delays.

3. Loss of control
   a. Unless we can negotiate it into the contract, we will lose many abilities that we have today to directly access logs, servers and potentially data.
   b. Cloud providers often upgrade all clients at the same time. What notice do we need and what works for us? This issue can be handled with the Terms and Conditions within a specific vendor contract.
   c. Staffing skills or the profile of staff will be impacted by any move to Cloud services. The network team and database management team members currently maintain all hardware and software for the College. This on-premise management would change into a remote oversight job which would require a new skill-set, one that dictates a security focus.
   d. Additionally, the potential for a breach of boundaries and theft of data is higher when sharing the same space (multi-tenancy) model
4. Availability
   a. Availability assurances are stated in Service Level Agreements or SLAs. These SLAs must be in place to help mitigate downtime; however, unexpected down time does occur. What is the cost of being down and how is the College compensated for the loss of service?
   b. The second availability issue is Response Time. This directly relates to performance issues of not just the system but of the productivity of the business units utilizing the system. Sluggish response can be as detrimental as down time during peak-times of activity for the College.
5. Ability to integrate
   a. Can we get seamless integration on demand? What would this entail; availability of an integration strategy that includes tools that enhance the Cloud application to perform as expected when integration with another service or platform is required.
6. Lack of ability to customize
   a. A configurable Cloud. The biggest challenge the College has faced with our ERP implementation is the constant requests to modify the base-line

code of Banner. In choosing a Cloud host we would look for a vendor that not only supports customization but demands certain standards. These standards may lock the College into certain system variables that cannot be changed thus causing a change in our business process.

7. Fiscal stability of cloud service provider. As stated earlier, the financial viability of any Cloud provider must be taken into consideration.
8. Does the provider use a multi-tenancy architecture? This also ensures that the provider is keeping all customers at the same software release; leaving no one behind. This offers distinct cost advantages.
9. Regular, managed software updates. Software updates should be handled multiple times per year and at no cost to the College. If the College chose to manage updates, it would be our cost so we would have to ensure that thorough testing is done prior to a production implementation.
10. Provide a sustainable, high-performance infrastructure. Any Cloud provider should provide a high-performance infrastructure that consists of databases, operating systems, networks, and storage systems used to run and deliver the Cloud applications.
11. Provide a predictable Total Cost of Ownership (TCO). This means no surprise costs. From implementation forward no costs should be a surprise. Hardware and software license fees should not require upfront investments.
12. Fast deployment. This corresponds the time and effort needed for in-house deployments. In a multi-tenant, configurable cloud, the testing of a new deployment then release should be days not months.
13. Control. Cloud applications should provide the College with complete control of our data as if the data remained on-site. The switch to a hosted application can become a challenge to data control. By data control we are referencing the need to search the past for e-Discovery.

Factors in Total Cost of Ownership (TCO)

Organizations looking to the cloud should evaluate their total cost of ownership. Some of the benefits that draw organizations to look to the cloud are scalability and efficiency. The pay-as-you-go model sounds appealing, but, how do organizations consider what resources they are using so that they can truly compare the two models for cost efficiency? There are a number of TCO calculators offered by cloud service providers or by other organizations supporting the cloud initiative to assist organizations with this. While there is no single standard evaluation, there are a number of factors that we believe must be considered. Total cost is comprised of many sources, including, but not limited to:

- The actual purchase cost of the hardware and software application.
- The indirect and direct costs necessary to support running the server and application[ix].
    - This includes electricity, floor space, storage, network infrastructure, ongoing support contracts and licensing, support personnel, personnel to secure the hardware and software.

- The cost to support business continuity and disaster recovery processes for the server and application.
- The indirect cost of having complete control of the hardware and application environment.
- The effect that load variation might have on cost in a pay-as-you-go model. With ownership, resources are secured and paid for entirely, regardless of utilization. Tracking utilization levels provides the necessary information to understand how a pay-as-you-go model can affect potential costs.

Next Steps

Is the College ready to move to the cloud? The truth lies in the total cost of ownership of any such move and the College's ability to accept the risk that comes with the cloud. Does the current investment in hardware, software and talent for managing our systems provide for a reduced cost of ownership that will deliver the needed services for the College?

Security of data is the prime concern since we hold so much information about our employees and students. Intrusion into a local database is a risk that is lessened by the controls in place by trained staff and reliable monitoring services. Currently, the College can state that we have never had an intrusion that put PII (personal identifiable information) at risk.

Taking a pragmatic approach to Cloud provider selection seems the safest path for the College. To that end we have chosen to move a few more services outside into a PaaS Cloud solution; Resource25 and OnBase Document Imaging. In addition, Institutional Advancement will begin using Nex Gen web Solutions Scholarship Processing system.

The criteria for the selection:

- Personal Identifiable Information is minimal or well protected.
- Hosting services are available and well tested.
- Services are NOT mission critical.
- In 2 of the 3 cases, IT staff members are overburdened by the support of these applications. Hosting will focus these efforts on critical support in lieu of constant hardware/software solution battles.

Resource25 as a hosted solution February 2012

Collegenet will host their scheduling solution software which we are going live with for event and classroom schedule management in the Spring of 2012. The new release, 25Live, will provide more functionality and flexibility for scheduling in addition to being a totally hosted solution for the College. This solution was chosen in part due to the non-PII data contained in the application as well as staff time and hardware costs associated with this application over the years.

OnBase Document Imaging as a hosted solution – February 2012

The hosted solution for OnBase will free the College of the hardware cost of this solution thus decreasing costs and increasing the efforts toward a greener environment.

Nex Gen Web Solutions – Scholarship Management – January 2012

Scholarship Manager provides a comprehensive solution to your Scholarship process. From online applications through online review and awarding, Scholarship Manager can help you automate and simplify your scholarship process.

Key features include:

- **Automated Matching** – Review only those candidates that qualify for a scholarship. Match qualified students to available scholarships using verified and self-reported data.
- **Simple application** – simplify the process for your students by removing the need to complete multiple applications.
- **Centralized process** - Scholarship Manager allows you to centralize the scholarship management process for your institution, but still decentralize the decision making process!
- **Reliable, scalable, secure** – Scholarship Manager is a cloud based solution that allows you to focus on the task at hand without having to worry about IT infrastructure and support.

---

[i] Black, Mandelbaum, Grover, Marvi (2010, November). The Arrival of Cloud Thinking. Retrieved August 1, 2011 from http://resources.idgenterprise.com/original/AST-0025847_The_Arrival_of_Cloud_Thinking_.pdf.

[ii] Mell, Peter and Tim Grance. (2009, October 7). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology*.Retrieved August 5, 2011, from http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[iii] Multitenancy. (n.d.). In *Wikipedia*. Retrieved August 19, 2011, from http://en.wikipedia.org/wiki/Multitenancy

[iv] Wainewright, Phil. June 20, 2008. Why multi-tenancy matters. *ZDNet*. Retrieved August 19, 2011, from http://www.zdnet.com/blog/saas/why-multi-tenancy-matters/537?tag=content;siu-containe0072.

[v] Cloud Deployment Methods. *Cloud Computing Consulting*. Retrieved August 19, 2011, from http://www.cloudconsulting.com/deployment-methods/.

[vi] Dunlap, Charlotte. June 16, 2010. Why Microsoft's Hybrid Cloud Threatens Google. *Forbes.com*. Retrieved August 19, 2011, from http://www.forbes.com/2010/06/16/microsoft-google-cloud-technology-azure.html.

[vii] Brodkin, Jon. July 2, 2008. Gartner: Seven cloud-computing security risks. *InfoWorld*. Retrieved August 30, 2011, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1.

[viii] Cloud Service Legal Issues – Data Privacy, Data Location and Secondary Use of Data. (June 20, 2011). Retrieved September 2, 2011, from http://www.channelprosmb.com/article/24800/Cloud-Services-Legal-Issues-mdash-Data-Privacy-Data-Location-and-Secondary-Use-of-Data/;jsessionid=F98243644CEA62C73D9978ED91B48234?textpage=2.

[ix] Cloudonomics: The Economics of Cloud Computing. (2011). Retrieved on September 2, 2011, from http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Cloudonomics-The_Economics_of_Cloud_Computing.pdf.

OTHER REFERENCES

Cloud Security Alliance. December 2009. "Security Guidance for Critical Areas of Focus in Cloud Computing v2.1". Retrieved on September 2, 2011, from https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.