2012 CACUBO Annual Meeting

Cloud Computing – The Next Big Thing in IT and Its Implications for Higher Education

Mark Oster
Partner-in-Charge,
Business Advisory Services
National Not-for-Profit Practice

Jill Albin-Hill
Chief Information Officer
Dominican University
Agenda

• Background
• Cloud Computing Overview
• Risks and Audit Strategies
• Summary
• Group Discussion
• Questions/Comments
Background

Separating Hype from Reality – What’s New?

• In some respects, not that different from services that have been used by businesses for years
  – ADP as a “software-as-a-service” (SaaS)

• New combinations of existing tools, some new technologies, and some very significant marketing

• It’s “Back to the Future”
  – From service bureaus to ASPs

• But it is here to stay
  – Virtual resource allocation and real-time performance optimization yield significant benefits
Background

Cloud Computing – A Force

• Gartner Survey of 2,000+ CIOs: top technology priority for 2011

• IDC: The market for cloud-computing is expected to grow more than 27% annually over the next five years and reach $73B by 2015

• IDC: By 2015, one of every seven dollars spent on technology will be connected with cloud computing

• Forrester: Cloud computing is a sustainable long-term paradigm and the successor to previous mainframe, client/server and network computing eras
Background

Cloud Computing – A Force
Background

Cloud Computing – A Force

• *The Big Switch* by Nicholas Carr – equating the significance of the shift to cloud computing in the information age to electrification in the industrial age
  
  – A hundred years ago, companies stopped generating their own power with steam engines and dynamos and plugged into the newly built electric grid. Today, a similar revolution is under way. This time, it’s computing that’s turning into a utility.
  
  – Cheap, utility-supplied computing will ultimately change society as profoundly as cheap electricity did. We can already see the early effects -- in the shift of control over media from institutions to individuals, in debates over the value of privacy, in the export of the jobs of knowledge workers... As information utilities expand, the changes will only broaden, and their pace will only accelerate.
Background

Why the buzz?

- Cloud computing is the future of IT
  - A new and flexible model for deploying technology
  - Extremely reliable and infinitely scalable
  - Strong cost/benefits and ease of ownership
  - Allows you to expand or contract as business needs dictate
  - Pay for only what you need at any given time and only for the duration you need it
The term “cloud” originated as a metaphor to depict the public switched telephone system on network diagrams.
Overview

What is Cloud Computing?

• An alternative to mainframe and client-server technology
  – The old: Fixed capacity requires investment in infrastructure beyond immediate/current needs
  – The new: On-demand, at-scale access to software, infrastructure and development tools

• Computing processing, infrastructure, applications, etc. all delivered as a service – wherever and whenever needed
Overview

What is Cloud Computing?

• Architecture (can be hosted internally or by a third-party)
  – External/Public
  – Internal/Private
  – Hybrid

• Service Types
  – Infrastructure-as-a-Service (IaaS)
  – Platform-as-a-Service (Paas)
  – Software-as-a-Service (SaaS)
  – Desktop-as-a-Service (DaaS)
  – Business Process-as-a-Service (BPaaS)

The “big 3”
Overview

Architecture - External/Public

- **Shared** computer resources provided by an off-site third-party provider
- Pay-per-use access to data, applications, infrastructure, etc.
- Examples
  - CRM (e.g., Salesforce.com)
  - Productivity tools (e.g., email from Google or Microsoft)
  - Data storage (e.g., Amazon, Barracuda)
## Overview

### External/Public - Economics

<table>
<thead>
<tr>
<th>Factor</th>
<th>On-premise</th>
<th>Cloud computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expenditure type</td>
<td>Capital expenditure (capex)</td>
<td>Operating expense (opex)</td>
</tr>
<tr>
<td></td>
<td>Operating expense (opex)</td>
<td></td>
</tr>
<tr>
<td>Cash flow</td>
<td>Servers and software are purchased upfront.</td>
<td>Payments are made as the service is provided.</td>
</tr>
<tr>
<td>Financial risk</td>
<td>Entire financial risk is taken upfront, with uncertain return.</td>
<td>Financial risk is taken monthly and is matched to return.</td>
</tr>
<tr>
<td>Income statement</td>
<td>Maintenance and depreciated capital expense</td>
<td>Maintenance expense only</td>
</tr>
<tr>
<td>Balance sheet</td>
<td>Software and hardware are carried as a long-term capital asset.</td>
<td>Nothing appears on the balance sheet.</td>
</tr>
</tbody>
</table>
Overview

Architecture - Internal/Private

• **Dedicated** computer resources provided by an off-site third-party, or use of cloud technologies on a private internal network

• Internal clouds
  – managed by in-house IT staff
  – physical infrastructure and data stored/maintained on-site
  – access via Internet or local network
  – differs from LAN/WAN due to consolidated infrastructure and processing, along with virtual allocation of resources
Overview

Architecture - Internal/Private

• Examples
  – ERP (e.g., SAP, Blackbaud)
  – Productivity tools (e.g., Sharepoint, Exchange Webmail)
Overview

Architecture - Hybrid

• Consisting of **mixed-use multiple** public/private clouds
• Integrates on-site IT infrastructure and internal cloud applications with third-party provider services
• Mission-critical processes maintained on-site
• Examples
  – Outsourced payroll; in-sourced membership management
Overview

Infrastructure-as-a-Service

• Computer infrastructure delivered over the Internet (e.g., Amazon, Rackspace)

- Infrastructure Provided
  - Data Center
  - Processor
  - Memory
  - Storage
- Virtualized & Dynamic
- Redundant/Hardened
Overview

Platform-as-a-Service

• Full or partial operating system/development environment delivered over the Internet, supporting online access and collaboration and access to a robust toolset (Amazon’s Elastic Beanstalk, MS Azure, Google App Engine)
Overview

Software-as-a-Service

- Software applications delivered over the Internet (e.g., Salesforce, Netsuite, Google Apps, DeskAway)
Overview

Service model attributes

• Software-as-a-Service (SaaS)
  – The consumer does not manage or control the underlying cloud infrastructure, platform, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

• Platform-as-a-Service (PaaS)
  – Consumer has control over the deployed applications and possibly application hosting environment configurations

• Infrastructure-as-a-Service (IaaS)
  – Consumer has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers)
Overview

DaaS and BPaaS

- Desktop-as-a-Service
  - Provides desktop virtualization for single user clients
  - Allows access to an individual workstation, as well as its operating system and storage hardware, via the Internet
  - Example: GoToMyPC

- Business Process-as-a-Service
  - Similar to SaaS, but rather than applications, the cloud provider hosts specific business processes, such as employee benefits management, help desk, or procurement to multiple internal or external customers
  - Example: Telegenisys and Wipro
Overview

Global Public Cloud Market Size

[Graph showing the growth of the total public cloud markets (US$ billions) from 2008 to 2020.]
Overview

Benefits

• Cost Effective and Higher Utilization of Resources
  – Dynamic allocation as needed
  – Dynamically de-provision when not needed (released back into a common pool for reallocation to others)

• Speed to Deployment
  – Enable faster delivery of applications and upgrades
  – Rapid deployment of infrastructure, platform modifications, etc.
Benefits

• Operating and Capital Cost reduction
  – Pay-per-use model more accurately matching organizational need (reduced capital for future capacity)
  – Lower energy use and facility costs
  – Lower maintenance and personnel costs

• Performance
  – Scalability to support growth or peak usage needs
  – More efficient and effective system-wide deployment of applications
  – Enhanced interoperability of disparate hardware/software
Risks and Audit Strategies

In the news…

• System failure at Amazon.com
  – “A widespread failure in Amazon.com’s Web services business affected many Internet sites, highlighting the risks involved when companies rely on so-called cloud computing…” – NYTimes.com April 21, 2011

• Security breach at Epsilon
  – “A data breach at one of the world's largest providers of marketing email services may have enabled unauthorized people to access the names and email addresses for customers of major financial-services, retailing and other companies…” – WSJ.com April 4, 2011
Risks and Audit Strategies

Key risk areas

- **Data security and controls** - third party reliance, compounded by exposure to the Internet
- **Regulatory** – dependence on knowledge of and compliance with industry specific requirements
- **Multi-tenancy** – concern regarding co-mingling of and/or access to data
- **Data location** – uncertainty regarding physical location of institutional assets
- **Reliability** – availability of resources when needed
- **Sustainability** – disaster recovery/business continuity
Risks and Audit Strategies

Data Security and Controls – Risks

• The cloud provider’s security policies and internal controls are not as strong as the institution’s requirements
• Cloud systems which store institutional data are not updated or patched when necessary
• Security vulnerability assessments or penetration tests are not performed to ensure logical and physical security controls are in place
• The physical location of company data is not properly secured
Risks and Audit Strategies

Data Security and Controls – Audit Strategy

• Determine cloud provider’s security and control practices
  – Is a SSAE 16 (formerly SAS 70) available and are all control concerns addressed?
  – Does contract contain a right to audit clause?
• Is there a SLA with minimum control standards specified?
• Determine if the cloud provider’s security posture is based on a security standard (e.g., ISO27001, Cloud Security Alliance, PCI DSS, etc.)
• Determine if the cloud provider has had a security assessment performed
Risks and Audit Strategies

Regulatory – Risks

• Does vendor comply with industry and legal standards (PCI, HIPAA, etc.)?
• Are state privacy laws (MA, CA, etc.) upheld?
• Is data stored in international locations, thereby falling under foreign business or national laws/regulations?
Risks and Audit Strategies

Regulatory – Audit Strategy

• Inquire as to vendor’s approach for compliance
• Request attestation
• Check contract terms for inclusion of specific regulatory adherence
• Inquire as to practices regarding provider’s approach to maintaining regulatory compliance if data resides in multiple locations
Risks and Audit Strategies

Multi-tenancy – Risks

- Institutional data is not appropriately segregated on shared hardware, resulting in data being inappropriately accessed by third parties
- The cloud service provider has not deployed appropriate levels of software control to ensure data is appropriately segregated, both in rest and transit
Risks and Audit Strategies

Multi-tenancy – Audit Strategy

• Inquire as to the cloud service provider’s method used to secure data from being accessed by other customers/third parties
• Review independent audit report(s) and/or exercise the institution’s right-to-audit clause
• Gain access to cloud system(s) and perform limited auditing procedures from the institution’s location
Risks and Audit Strategies

Data Location – Risks

- The institution does not know where their data is physically or virtually stored
- The institution is not aware of all of the cloud service provider’s physical location(s)
- The cloud service provider moves data to another location without informing the institution
- If the institution chooses to migrate all or part of its system and/or data back in-house (or to another provider), the cloud service provider cannot (or will not) provide the data
Risks and Audit Strategies

Data Location – Audit Strategy

• Inquire of the cloud provider the specific physical and virtual location of the institution’s data

• Work with your legal group to fully understand the impact and potential risks of data residing in a foreign country

• Determine if the contract provides for the institution to move data back in house and/or to another provider, and determine the specific procedures and associated costs needed to perform this task
Risks and Audit Strategies

Reliability – Risks

- Are quality of service standards consistent with identified business requirements regarding availability?
- Will resources scale as expected during peaks?
- Concentration of resources – potential single point of failure
- Vendor viability
  - In the event the cloud service provider goes out of business, the institution might not be able to sustain operations or retrieve its data
  - Another third party might gain access/control of the institution’s data
Risks and Audit Strategies

Reliability – Audit Strategy

• Understand the cloud provider’s approach to scale its systems to meet short-term spikes and long-term growth

• Compare SLA/contract specifications to actual performance

• Determine the times that the cloud provider performs system upgrades and/or patches to ensure data availability during peak business hours is not affected

• Determine means for gaining access to data in the event the cloud service provider goes out of business

• Review vendor financials
Risks and Audit Strategies

Sustainability – Risks

- The cloud service provider does not have appropriate system recovery procedures in place in the event of a disaster
- The institution’s business continuity plan does not address the cloud’s service offering being unavailable
- Institutional data is compromised as a result of a disaster
Risks and Audit Strategies

Sustainability – Audit Strategy

• Inquire to determine if the cloud provider has adequate controls in place to protect and recover data in the event of a disaster

• Review the institution’s business continuity plan and determine if the plan establishes standards for allowable downtime and addresses interruptions with the cloud solution in the event of a disaster

• Perform a service disruption test for appropriateness and timeliness of response
Summary

Considerations

- Fundamentally, it’s as much an outsourcing decision as it is a technology decision
  - Alignment with short and long term IT strategy
  - Business partner reliability, integrity, etc.
  - Service level (uptime, recoverability, support, escalation)
  - Confidentiality, privacy, security, compliance
  - Standardization of services vs. customized fit
  - Ability to “unwind” the relationship – return or transfer
  - Can’t outsource your responsibility or your problems
Summary

New Clouds are Rolling in Daily...Are you ready?
Questions/Comments
Contact information

Mark Oster
Partner-in-Charge,
Business Advisory Services
National Not-For-Profit & Higher Education Practice
T 212.542.9770
E Mark.Oster@us.gt.com

Jill Albin-Hill
Chief Information Officer
Dominican University
T 708.524.6980
E jalbin@dom.edu