Cloud Computing Discussion
Presenters
RICHARD ARCHER

Rich is a partner in KPMG’s Advisory Services Practice based in Pittsburgh. Rich has assisted clients in areas related to IT, risk management, process analysis and improvement, security analysis, IT PMO, control analysis and enhancement, and business process transformation. He has been a member of the MidAtlantic Advisory leadership team, National IT Audit leadership team, National Business Continuity leadership team, as well as having been a member of the National Sarbanes Oxley development team. Currently Rich is the partner in charge of the Pittsburgh IT Advisory group.

Prior to joining KPMG, Rich was the supervisor of data security and disaster recovery for Duquesne Light Company. He established the IT audit function at Allegheny General Hospital, and was promoted to the position of Director, HRIS. In addition, he has also held positions in IT for several Pittsburgh area companies.

Rich has displayed a history of increasing responsibility and development of personal skill sets, along with development of practice capabilities and business expansion. He has acted as both a regional and national resource for key service opportunities. In addition, Rich has been a marketplace leader in the development of focus account relationship and business opportunity penetration.

Rich was an initial attendee of the KPMG Advisory International Partner Information Share Forum and he has attended the KPMG Lead Partner Academy.
JUSTIN J. WEISSERT

Justin is a manager in KPMG’s IT Advisory Services practice in Pittsburgh, PA. Justin has more than four years of advisory and business experience. He has a strong background in both advisory and attestation engagements focused on financial, insurance, and pharmaceutical companies. Justin's current and past clients include some of the leading entities in these industries.

Justin has experience as a leader of several IT advisory engagements of various sizes across several industries, with a focus on the financial services, insurance, and pharmaceutical sectors. He manages and performs Identity and Access Management services including access governance strategy, roles based access controls (RBAC), access certification, access request, identity in the cloud, and project management. He also has experience with information security projects including penetration testing, information security governance strategy, vendor assessments, and third party access.

Prior to moving into the Information Protection space, Justin served as lead staff on attestation engagements. His primary focus had been on providing SAS 70 reporting and Sarbanes-Oxley 404 testing of IT systems.

Justin has a BBA in Management Information Systems from the University of Notre Dame.
Agenda

- Understanding Cloud Computing
  - Characteristics
  - Platforms and Deployment Models
  - Impact on Business
  - Use Cases & Trends for Cloud

- Statistics on Cloud Adoption
  - Highlights from KPMG’s Global Cloud Study
  - Migrating to the Cloud Model

- Benefits and Considerations

- Role of Internal Audit

- ISACA and KPMG Resources

- Q&A
Understanding Cloud Computing

There are several definitions of Cloud Computing. The National Institute of Standards and Technology (NIST) provides the following definition:

“Cloud computing 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.”

Cloud computing has five essential characteristics:

- **On-demand self-service**: Get it when you need it
- **Measured service**: Pay for what you use
- **Rapid elasticity**: Increase and decrease capacity quickly
- **Broad network access**: Access it from any Internet connection
- **Resource pooling**: Share fixed costs, which lowers individual costs

(Source: NIST 2009)
Understanding The Cloud Operating Environment

Cloud Environment = Internet-based data access & exchange + Internet-based access to low cost computing & applications

Cloud Environment Characteristics:
- Self-Service On-Demand
- Internet Accessibility
- Pooled Resources
- Elastic Capacity
- Usage-Based Billing

Cloud Service Models:
- Software as a Service ("SaaS")
  Business operations over a network
- Platform as a Service ("PaaS")
  Deploy customer-created applications to a cloud
- Infrastructure as a Service ("IaaS")
  Rent processing, storage, network, other computing resources

Cloud Deployment Models:
- Private
  Operated for a single organization
- Public
  Available to the general public or large industry group, owned by an organization selling cloud services
- Community
  Shared by several organizations, supporting a specific community
Cloud Impact on Business

Cloud Environment = Internet-based data access & exchange + Internet-based access to low cost computing & applications

Virtualized Technology

Virtualized Processes

Opportunities to Leverage Commoditized Enterprise Applications and Economies of Scale

Virtualized Business Models

- Increased Agility
- Greater Flexibility
- Faster Results
- Reduced Cost
Cloud and SaaS Will Permeate The Entire Value Chain

Planning
- Collaborative planning
- Demand/supply alignment
- Incremental planning

Procurement
- Automated procurement
- Sourcing, auctions, events
- Buy-sell, price masking

Manufacturing
- Co-manufacturing
- WIP visibility
- Quality management

Engineering
- Collaborative design
- Release management
- BOM Mgt/costing

Execution
- Vendor Managed Inventory
- POS Replenishment
- Order Management

Back Office
- Finance/HR
- Knowledge Management
- Team collaboration

Logistics
- Transportation mgt.
- Track and trace
- Logistics optimization

Sales & Revenue
- Customer management
- Order tracking
- S&OP
KPMG and Forbes Insight conducted a global survey in 2011 among more than 900 individuals from 15 countries worldwide regarding the cloud and some of the results are highlighted below:

<table>
<thead>
<tr>
<th>Highlight</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>81%</td>
<td>Businesses are either planning their initial forays, are in early stages or advanced stages of experimentation or have full implementations.</td>
</tr>
<tr>
<td>Over half</td>
<td>Businesses and government enterprises have already conducted either a full (24%) or partial (35%) cloud implementation of some functions.</td>
</tr>
<tr>
<td>Typical areas</td>
<td>Cloud implementation are for email, sales management, and other Software as a Service (SaaS) offerings.</td>
</tr>
<tr>
<td>1 in 10</td>
<td>Businesses say they are already running their core IT services using cloud.</td>
</tr>
<tr>
<td>30%</td>
<td>While most providers promote up to 30% savings, most business executives would be happy with 10%-15% savings.</td>
</tr>
<tr>
<td>Most intriguing aspects</td>
<td>Speed to solution, widespread accessibility, flexibility, scalability, security, and advanced technology.</td>
</tr>
<tr>
<td>45%</td>
<td>Approximately 45% of the respondents are either not evaluating the tax implications of cloud or don’t know if these factors are being evaluated.</td>
</tr>
</tbody>
</table>

Respondents were from both the client community of end-users, with input from both IT directors and executive management in companies with more than US $200m in revenues, and cloud vendors.
The majority of CIOs plan to increase their usage of all cloud services over the next three years.

<table>
<thead>
<tr>
<th>Plans to Use Cloud Services</th>
<th>Currently Using, Actively Researching, Planning to use in one to three years</th>
<th>Planning to use three to five years</th>
<th>No plans to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application platforms and development software</td>
<td>68%</td>
<td>2%</td>
<td>30%</td>
</tr>
<tr>
<td>Collaboration tools</td>
<td>79%</td>
<td>4%</td>
<td>17%</td>
</tr>
<tr>
<td>Enterprise application software</td>
<td>63%</td>
<td>3%</td>
<td>34%</td>
</tr>
<tr>
<td>Personal productivity software</td>
<td>53%</td>
<td>4%</td>
<td>43%</td>
</tr>
<tr>
<td>Utilities/management software</td>
<td>66%</td>
<td>2%</td>
<td>32%</td>
</tr>
<tr>
<td>Networks</td>
<td>52%</td>
<td>2%</td>
<td>45%</td>
</tr>
<tr>
<td>Storage</td>
<td>63%</td>
<td>7%</td>
<td>30%</td>
</tr>
<tr>
<td>Servers</td>
<td>59%</td>
<td>2%</td>
<td>39%</td>
</tr>
</tbody>
</table>


*<http://www.cio.com/article/455832/Cloud_Computing_Survey_IT_Leaders_See_Big_Promise_Have_Big_Security_Questions?page=3&taxonomyId=3112>
Cloud Computing Benefits

Cloud computing offers significant general benefits

- Allows companies to focus on core missions
  - A recent survey of IT managers found that server management tasks consumed one-third of IT staff time.
- Increased agility in software deployment
  - Reduced time to provision software testing/development space
- Increased productivity
- Easy and low-risk to test drive cloud applications (compared to in-house software products)
- Shift from capital expenditures to O&M expenditures; significant hardware savings
- More IT organization focus on supporting the mission, less focus on technology

Cloud computing can help agencies reduce IT costs.

- Average server utilization is 15%
- $800 billion spent yearly on purchasing and maintaining enterprise software
- IT operation costs are high, and growing
  - Current $76 billion federal IT budget; infrastructure accounts for one half of this
  - 2006 estimate: Federal servers and data centers alone account cost $450 million annually.
- Some organizations have saved 50-90% by shifting to the cloud

Sources:
Cloud Computing Benefits

Energy Savings and Environmental Benefits

- Data centers are energy intensive.
- A data center’s IT equipment alone can use between 10 and 100 Watts per square foot of raised floor area.
- Data centers can consume up to 100 times more energy than a standard office building.
- Data centers consumed 61 billion kilowatt-hours of power in 2006 (equal to 1.5% of all power consumed in the United States).
  - Federal servers and data centers alone account for 6 billion kWh (10%) of this use,
  - Under current trends, the federal government’s peak load for servers and data centers could near 1.2 GW and cost $740 million by 2011.
- IT produces 2% of global carbon dioxide emissions.

Sources:
Adopting cloud has considerable impact on Information Technology (IT), but it doesn’t stop there. Beyond IT implications, critical business operations such as financial management, tax, regulatory compliance, vendor management, security & privacy and a host of other areas get impacted too.
Key Risks & Challenges in Adopting Cloud

- Cloud adoption requires a careful examination of the potential technology and operational risks and challenges. Some of the key business operation challenges an enterprise could face are illustrated below:

**Financial & Tax**
- Movement from CapEx to OpEx model impacts existing budgeting, forecasting and reporting processes
- CapEx to OpEx model and changes in the character and source of service impacts tax considerations
- ROI and cost/benefit analysis of cloud is dependent on knowledge of existing cost of delivery as well as future usage of service, makes it a complex model

**Security and Privacy**
- No control over critical security areas such as vulnerability management, infrastructure hardening, or physical security
- Weak logical access controls due to cloud vendor’s IAM immaturity
- Data may physically reside in a legal jurisdiction where the rights of data subject are not protected

**Vendor Management**
- Lack of clarity on ownership of responsibilities between cloud vendor and user company
- No prevalent standards for vendor interoperability
- Extensive reliance on the Service Provider

**Operational**
- Cloud sourcing makes some existing organizational roles and skills redundant
- Cloud adoption introduces rapid change in the organization
- Business resiliency/disaster recovery needs and plans gets impacted

**Information Technology**
- Cloud adoption opens the four Data Center walls to external IT Services providers, creating new risks
- Business can bypass the IT function to implement technology solutions, making IT governance challenging
- Cloud delivery models dramatically changes the paradigm for how IT delivers technology services to support business requirements
- Risk of creating independent silo of information

**Regulatory and Compliance**
- Lack of visibility into cloud provider’s operations to analyze how various laws, rules, and regulations that apply to an organization are complied with
- Complexity of records management/records retention
- Lack of industry standards and certifications for cloud providers
Considerations for Operating in Cloud - Security & Privacy

### Challenges / Implications

- No control over critical security areas such as vulnerability management, infrastructure hardening, or physical security
- Weak logical access controls due to cloud vendor’s IAM immaturity
- Data may physically reside in a legal jurisdiction where the rights of data subject are not protected

### Considerations

- **Data Governance:** A well thought out data/information governance program can help with smooth cloud deployments. Classify data and applications and identify encryption, co-location, and policy requirements prior to adopting cloud.
- **Data Access:** Develop a framework for sharing user identities and user access to sensitive data at the CSP; Define conditions under which third parties, including government agencies, might have access your data at the CSP.
- **Security Risk Assessment (SRA):** Develop a robust risk assessment model to identify and evaluate security and privacy risks and the impact of using a Cloud Service Provider (CSP). Reevaluate risks on an ongoing basis.
- **Security Requirements:** In absence of a standard security practices across the cloud providers, clearly articulate and define your cloud security requirements; and develop a strong security contract/SLA.
- **Privacy:** Evaluate CSP practice of collection, maintenance, use, and disclosure of personally identifiable information (PII). Defining circumstances under which any PII can be shared or disclosed by CSP.
## Considerations for Operating in Cloud - Operational

### Challenges / Implications

- Cloud sourcing makes some existing organizational roles and skills redundant
- Cloud adoption introduces rapid change in the organization
- Business resiliency/disaster recovery needs and plans gets impacted

### Considerations

- **Roles & Responsibilities**: To reduce confusion regarding who is providing which IT services, the company or the CSP, invest time upfront to define and agree to specific roles and responsibilities. Also, the existing IT skills would need to shift from performing IT operations to managing and interfacing with CSP.

- **Human Capital**: Resource impacts are often overlooked until skill sets are impacted by loss or changes. Taking a strategic view of human capital during migration planning is critical to the success of any large-scale cloud deployment.

- **Change Management**: With the rapid deployment capability of cloud computing services, the issue of change management needs to be considered carefully. When it becomes too easy to deploy or modify an application in the cloud, control might be overlooked.

- **Business Continuity/Disaster Recovery**: Review and update your business continuity plans to ensure that you will get your business operational if your cloud provider suffers a disaster. Also look at leveraging cloud based DR solutions for your internal infrastructure and applications.
## Considerations for Operating in Cloud - Information Technology

### Challenges / Implications

- Cloud adoption opens the four Data Center walls to external IT Services providers, creating new risks
- Business can bypass the IT function to implement technology solutions, making IT governance challenging
- Cloud delivery models dramatically changes the paradigm for how IT delivers technology services to support business requirements
- Risk of creating independent silo of information

### Considerations

- **Technology Strategy & Architecture**: Work closely with business and define upfront a clear vision and cloud strategy with a long-term view of technology architecture principles and standards in order to ensure interoperability, data integration, security and controls across the myriad of providers.

- **Service Catalog**: To reduce the risk of business units circumventing corporate functions and IT when deploying cloud solutions, consider centralizing the cloud computing initiative across the company and provide service offerings to the business through a single-service catalog

- **IT Governance**: New governance models and compliance strategies are needed to enable visibility into the organization’s risk exposure and effective decision making. Evolve IT governance structure and governing bodies to include vendor executives in the IT eco-system.

- **IT Solution Delivery**: Traditional SDLCs must evolve into IT Services Integration Life Cycles models that support not only internally developed applications but also the evaluation, adoption and integration of Cloud based solutions into the Enterprise IT landscape.

- **IT Service Management**: Evolve IT operating models and processes to focus on broad IT Service Management capabilities and not technology management. With cloud, Service Levels, Service Demand and Service Capacity have become increasingly important.
## Considerations for Operating in Cloud - Regulatory & Compliance

### Challenges / Implications

- Lack of visibility into cloud provider’s operations to analyze how various laws, rules, and regulations that apply to an organization are complied with
- Complexity of records management/records retention
- Lack of industry standards and certifications for cloud providers

### Considerations

- **Collaborative Risk Assessment**: Internal audit, legal, risk, and security organizations should work closely from the start of any cloud computing initiative to identify potential regulatory and compliance risks early and incorporate them into the cloud computing business case.

- **Data Location**: Understand and include in contracts with CSPs where your data will be hosted and how required laws will be followed in those locations.

- **Breach and Disclosure**: The adoption of cloud requires changes in existing processes related to timely discovery, assessment, and reporting of the breaches from within the cloud in lieu of complying with regulations.

- **E-Discovery**: Using cloud computing services will not absolve a party from e-discovery responsibilities; it will just make them more challenging. Many CSP provide E-Discovery as an extra service, although it may cost more it may well be warranted to protect a company’s responsibilities for e-discovery.

- **Assurance**: The majority of CSPs will move to the SOC reporting model as a primary mechanism for providing assurance to their customers due to historical acceptance of the SAS 70 model and the cloud-focused criteria that underpin the SOC2 and SOC3 framework. Ensure that your organization understand the evolving assurance models.
### Considerations for Operating in Cloud - Vendor Management

#### Challenges / Implications

- Lack of clarity on ownership of responsibilities between cloud vendor and user company
- No prevalent standards for vendor interoperability
- Extensive reliance on the Service Provider

#### Considerations

- **Vendor Contracts**: Due to the lack of control that a user can enforce on the CSP, it is important to have a carefully define contract terms. Ensure that ownership of responsibilities, ownership of data, pricing, SLAs, right-to-audit clause, data import/export, etc. are clearly laid out in the contract prior to migrating data to a CSP.

- **Service Level Management**: Service Level Agreements (SLA) between providers and consumers is critical due to the dynamic nature of the cloud. Business should continuously monitor Quality of Service (QoS) attributes and enforce SLAs.

- **Vendor Management**: Centralize cloud computing vendor management; govern closely to prevent business units from circumventing IT and setting up their own cloud services.

- **Vendor Selection & Lock-in**: The viability of small cloud vendors could be a concern for long term continuity of service. Business will incur additional costs if they were to change CSP. Focus on performing a robust due-diligence before you select any CSP.

- **Billing Assurance**: As the business move away from paying one time license fees for software to subscription or usage based billing, it is important to build adequate controls in the payment process to ensure that they are not getting overbilled by the CSP.
## Considerations for Operating in Cloud - Financial Management

### Challenges / Implications

- **Movement from CapEx to OpEx model impacts accounting, budgeting, forecasting and financial reporting process**
- **ROI and cost/benefit analysis of cloud is dependent on knowledge of existing cost of delivery as well as future usage of service, makes it a complex model**

### Considerations

- **Accounting**: Movement from CapEx to OpEx model requires a review the existing accounting polices e.g., depreciation. Explore if there is a mechanism in GAAP/IFRS to capitalize a portion of cloud deployment cost.

- **Auditing**: As the data moves from residing within the company to outside, there is an increased reliance on third parties for supporting financial audits. Plan ahead, communicate the need for audit support to the cloud vendor and ensure that the contract with the vendor ensures such support.

- **Budgeting**: Plan for expense based budgetary process vs. capital based budgetary process. Identify what should leaders communicate to external stakeholders about the shift to cloud and its impact on the financial results and future estimates.

- **Forecasting**: To effectively calculate the ROI for the move to cloud and to continuously monitor the ROI, establish demand and capacity management internally to understand growth rates, forecast cloud service needs.
Cloud Computing – Internal Audit’s Role

- **Business Case and Vendor Due Diligence** – Assist management in the establishment of a business case for Cloud Computing and performance of due diligence for the service provider.
  - Has management established a defined business case, with expected returns, for the use of a Cloud Computing service provider?
  - Does management perform appropriate due diligence procedures when selecting a Cloud Computing service provider? If management identified potential risks with a selected Cloud Computing service provider, how does management mitigate those risks?

- **Legal and Compliance** – Work with general counsel and IT to determine if proper processes and controls are present.
  - How are the organization’s e-discovery requests handled for data stored in a Cloud Computing environment? Who has ownership of data stored in a Cloud Computing environment?
  - What are the organization’s legal and regulatory compliance impacts to using a Cloud Computing environment?
Cloud Computing – Internal Audit’s Role (continued)

- **Vendor Management** – Assess the vendor management function. Advise IT of associated risks when selecting a Cloud Computing service provider.
  - Does the organization have a strong vendor management function? How do Cloud Computing services affect the organization’s vendor management function?
  - How mature is the Cloud Computing service provider? Are there potential going concern issues?

- **Security and Privacy** – Perform security audits around Cloud Computing services.
  - How is security managed?
  - Does the organization have a robust and effective process for data classification and information life cycle management (i.e., is data classified as appropriate or not appropriate for sharing with third parties)?
  - How is data privacy maintained in a multi-tenant environment?

- **Availability and Performance** – Perform operational audits to determine if Cloud Computing services meet expected availability and performance metrics (e.g., SLAs) and if expected benefits are realized.
  - Do Cloud Computing services have guaranteed uptimes? What are the impacts to the organization if connectivity to Cloud Computing services is lost?
ISACA and Cloud Computing

- ISACA White Paper Guidance
  - ISACA White Paper: IT Control Objectives for Cloud Computing
    - [www.isaca.org/itcocloud](http://www.isaca.org/itcocloud)

- Additional KPMG Material
  - KPMG Institutes: “What You Should Know About Cloud Computing”
  - “Embracing the Cloud”

- “Clarity in the Cloud” – Executive Summary of KPMG’s Global Cloud Study
Q&A