Discussion Agenda

- Introduction to cloud computing
- Types of cloud services
- Benefits, challenges, and risks
- Questions for auditors
- Emerging good practices
- User auditor assurance – SOC1 /SAS 70 and SOC2 compared
- Auditing the cloud arrangement – A case study
- References
Tremendous Buzz Around Cloud Computing

“Spending on IT cloud services to grow almost threefold over the next five years”

Gartner EXP Worldwide Survey of 1600 CIOs

“Top barrier to cloud technology according to IT executives: Evaluating and managing security or business continuity risks”

McKinsey & Co. (November 2010)

“60% of virtualized servers will be less secure than the physical servers they replace through 2012”

Gartner Press Release – March 2010

“By 2012, 20 percent of businesses will own no IT assets”

Gartner’s top predictions for 2010 and beyond
What is Cloud Computing?

http://www.youtube.com/watch?v=bRi4vPO4DYY&feature=player_embedded
Cloud Service Model

- **Software as a Service (SaaS)**
  - Complete applications sold via subscription:
    - CRM, ERP, E-Mail, Calendar, Internet File Stores, Spam Filters…
    - E.g. GoogleApps, Microsoft Online Services

- **Platform as a Service (PaaS)**
  - Application building blocks:
    - Workflow, APIs, Proprietary Development Languages, Document Management, Data Services,
    - E.g. Google App Engine, Microsoft Azure

- **Infrastructure as a Service (IaaS)**
  - Core Infrastructure Services:
    - Operating Systems, Data Storage, Web Servers, Edge Caching Services
    - E.g. Rackspace, GoGrid, Amazon EC2
Cloud Deployment Models

- **Public**
  - Sold to the public
  - Owned by organization selling cloud services

- **Private**
  - Operated solely for an organization
  - May be managed by the organization or by a third party

- **Community**
  - Shared infrastructure for specific community concerns and benefits
Why Cloud Computing? …

The Benefits

- Pay-as-you-go model
- Scalable solution that supports rapid business growth
- Cost transparency to the end-user/business
- Lower time to market for IT solutions
- Outsourcing of competencies that are not core to the business
- No separate cost of tracking and installing Operating System patches
- Not limited to basic hosting of websites
Cloud Computing Challenges

- Vendor failures notably starts-ups
- Loss of physical control
- Security models and standards are still emerging
- ‘Who is responsible for what’ when a security breach happens
- Isolation/security between virtual machines
- Guest to host communication happens over the Internet
- Vulnerability of browsers
- Data privacy implications (e.g., data could be in another country)
- Availability concerns
- Implications for e-discovery
- Customer support practices are evolving
Inherent Risks in the Cloud Stack

- Data resides with the cloud provider
- Co-tenant can impact security
- Lots of configuration points
Questions for Auditors to Ask

- How much security is enough?
- Criticality of the application being sent to the cloud
- Outsourcer’s experience with SLA and vendor management
- Country/regional regulations (for e.g., SOX and Europe’s data privacy laws), and Industry Regulations (for e.g., GLBA and HIPAA)
- Does your present security model need to be altered?
- Cloud vendor’s policy on vulnerability management – reporting (beyond basic ‘Contact Us’ links), commitment to following up, promptly responding to reports etc.
- Is there an independent auditor’s report?
Some Emerging Good Practices

- Conduct a proper risk assessment before jumping into the cloud
- Store only non-private data in the cloud
- Data-at-rest encryption
- Document ‘who is responsible for what’
- Highly customized and transaction heavy applications are retained in-house
- Secure network connections for cloud administration
- Use more than one cloud provider or use provider with multi-location/country presence (depending on need)
- Auditing and Logging
Third-party Assurance

- Cloud Service provider relationships need ongoing monitoring
- Several attestation products are available
- One or more products may be relevant
- The attestation products serve as efficient means of obtaining ‘comfort’
## Comparison Between SAS 70/SSAE 16/SOC 1 Report and SOC 2 Report

<table>
<thead>
<tr>
<th></th>
<th>SAS 70 /SSAE 16 / SOC 1 Report</th>
<th>SOC 2 Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-established control objectives</td>
<td>No</td>
<td>Yes (Security, Confidentiality, Availability, Privacy, and Processing Integrity)</td>
</tr>
<tr>
<td>Scope exclusions</td>
<td>Privacy, business continuity and disaster recovery and any other subject matter not relevant to users’ financial statement assertions</td>
<td>No exclusions as long as it relates to one of the five key system attributes</td>
</tr>
<tr>
<td>Nature</td>
<td>Provides a report on the cloud provider’s controls related to financial statement assertions of user organizations</td>
<td>Controls over the security, availability and processing integrity of a system and the confidentiality and privacy of information processed by the system</td>
</tr>
<tr>
<td>Types of systems</td>
<td>Systems that process transactions or data for the user organization that are relevant for user organization’s financial statements</td>
<td>Systems that are not relevant /material for user organization’s financial statements but relevant for compliance and operations.</td>
</tr>
<tr>
<td>Distribution of report</td>
<td>Limited distribution report: User organizations and user auditors only</td>
<td>Limited distribution report: User organizations and user auditors only</td>
</tr>
</tbody>
</table>
Recap

- Use of cloud computing is expanding at a rapid pace
- Cloud computing has tangible business benefits
- Cloud computing leads to new risks
- Risks can be managed
- It can be a strategic differentiator
Auditing Cloud Computing Arrangements

How do We Audit the Cloud?
Cloud Outsourcing Lifecycle

Phase 1
Business Case

Phase 2
Vendor due diligence

Phase 5
Closing the relationship

Phase 3
Establishing vendor relationship

Phase 4
Ongoing monitoring
There are broad risk management frameworks such as COSO ERM
There are domain-specific frameworks such as ISO 27001 and ITIL
The Risk IT framework from ISACA fills the gap between generic risk management frameworks and domain-specific frameworks
IT risk is not purely a technical issue
The Risk IT framework is about business risk related to the use of IT
Linkage Between Risk and Controls

Top down
Risk scenarios:
Business Objective

Bottom up
Risk scenarios:
Generic scenarios

Combine and Refine

Refined and specific IT Risk scenarios

Risk Response

Risk Response Options

1. Avoid
2. Transfer
3. Mitigate
4. Accept
Background about the organization:

Organization ABC is a Healthcare provider (runs a network of hospitals and clinics), payer (Health Plan), and offers disease management solutions. It has recently outsourced the hosting of its data warehouse by utilizing an external cloud service provider (CSP) to host its data warehouse containing claims processing and summary health information for its care recipients and plan participants.

The CIO and CFO have engaged the internal auditor/co-sourced internal audit provider to conduct a review of the cloud computing arrangement.
Case Study Illustration

Figure 1 – Example of a Cloud Provider Setup and Users

Cloud containing Healthcare Data warehouse

- Healthcare organization’s sales rep. via PDA
- Employees of corporate clients accessing Claims History
- Disease Management specialists crunching treatment effectiveness ratios
- Messaging Server
- Laboratory Information Systems (data source)
- Claims Processing System (data source)
- Medical Records Servers (data source)
- Backup Administrator
- Healthcare Organization’s firewall separating it's internal network from the internet
## Risk-based Audit Scoping Utilizing RiskIT and COBIT

### COBIT processes and corresponding control objectives that influence all given Risk IT high-level risk scenarios

<table>
<thead>
<tr>
<th>Risk IT Ref # and corresponding High-level Risk Scenarios</th>
<th>Phases 1, 2</th>
<th>Phases 2, 3</th>
<th>Phase 3</th>
<th>Phases 4, 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Technology Selection</td>
<td>Plan and Organize (PO)</td>
<td>Acquire and Implement (AI)</td>
<td>Deliver and Support (DS)</td>
<td>Monitor and Evaluate (ME)</td>
</tr>
<tr>
<td>10. Regulatory compliance</td>
<td>PO 3.2</td>
<td>AI 1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Selection/performance of third-party suppliers</td>
<td>PO 5.5</td>
<td>AI 5.2</td>
<td>DS 2.4</td>
<td>ME 3.1</td>
</tr>
<tr>
<td>27. Logical Attacks</td>
<td></td>
<td>AI 2.4</td>
<td>DS 5.10, DS 5.3</td>
<td></td>
</tr>
<tr>
<td>28. Information Media</td>
<td></td>
<td></td>
<td>DS 5.11</td>
<td></td>
</tr>
<tr>
<td>31. Database Integrity</td>
<td></td>
<td></td>
<td>DS 11.6</td>
<td></td>
</tr>
<tr>
<td>32. Logical Trespassing</td>
<td></td>
<td></td>
<td>DS 5.4, DS 5.5</td>
<td></td>
</tr>
<tr>
<td>34. Contract Compliance</td>
<td></td>
<td></td>
<td></td>
<td>ME 3.4</td>
</tr>
</tbody>
</table>
References

● The Risk IT Framework from ISACA
  http://www.isaca.org/Template.cfm?Section=Risk_IT7&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749

● ENISA Cloud Computing: Benefits, Risks and recommendations for information security, November 2009

● Virtual Machine Security Guidelines by The Center for Internet Security

● Forrester Research "Database-as-a-Service Explodes on the Scene"

● Gartner Research http://www.gartner.com/it/products/research/cloud_computing/cloud_computing.jsp

● American Institute of Certified Public Accountants (AICPA)
  http://www.infoq.com/articles/nasdaq-case-study-air-and-s3;jsessionid=E61F6DC4D149E05B27C933F5F37312BA

● Cloud Security Alliance: Security Guidance for critical areas of focus in cloud computing v2.1


● McKinsey & Company – How IT is managing new demands (November 2010)
Presenter’s Contact Details

Sailesh Gadia
KPMG LLP
+1 (612) 305 5087
sgadia@kpmg.com
www.kpmg.com