Cloud Computing: Risks and Auditing

Phil Lageschulte/Partner/KPMG

Sailesh Gadia/Director/KPMG
Cloud Computing Overview
Cloud Computing Definition

Cloud Computing
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 is not:**
  - Any specific technology, such as VMware or SalesForce
  - Virtualization
  - Outsourcing
  - Grid computing
  - Web hosting

- **Cloud Computing is:**
  - An IT delivery approach that binds together technology infrastructure, applications, and internet connectivity as a defined, managed service that can be sourced in a flexible way
  - Cloud computing models typically leverage scalable and dynamic resources through one or more service and deployment models
  - The goal of cloud computing is to provide easy access to, and elasticity of, IT services.

**Characteristics of cloud computing include**

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Metered service

KPMG’s cloud computing definitions align with NIST working definitions.

*NIST National Institute of Standards and Technology Technology Administration, U.S. Department of Commerce*
Cloud Models

Private Cloud

A private cloud is a ‘closed’ network of computing resources dedicated to one organization, ‘single-tenant’. A private cloud can be internal or external.

**Private internal** cloud is where computing resources are owned and maintained by the organization’s own IT.

**Private external** cloud is where computing resources are owned and maintained by the service providers for a fee to the using organization.

Public Cloud

The cloud infrastructure is made available to the general public or a large industry group, ‘multi-tenant’, and is owned by an organization selling cloud services.

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications (and services) running on a cloud infrastructure.

Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
Impact of Cloud Computing on IT Operating Model

The Business

IT Service Integration Roles

- Service Owner
- IT Risk Manager
- Vendor Manager
- IT Finance Manager

Internal IT Organization
(non-cloud retained IT Services)

Service Ownership:
- Single Point of Contact with the CSPs & IT
- Demand Capture
- Services Standards
- Service Level Monitoring

IT Risk Mgmt:
- Risk identification and analysis across different CSPs
- Risk library
- Vendor/CSP Audits
- Compliance Monitoring

Vendor Mgmt:
- Vendor certification
- Contract Negotiations

IT Finance Mgmt:
- Business case
- Service Costing and Chargeback
- SLA penalty-bonus calculation

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.
Cloud Computing Risks and Audit Considerations
Dimensions of Risk

Operating in a Cloud Environment Presents Risks in Several Dimensions

**Identify and Access Management**
- User access provisioning
- Deprovisioning
- Super user access

**Financial and Vendor Management**
- Under-estimated start-up costs
- Exit costs or penalties
- Management over-head
- Run-away variable costs

**Regulatory**
- Complexity to ensure compliance
- Lack of industry standards and certifications for cloud providers
- Records management/records retention
- Lack of visibility into service provider operations and ability to monitor for compliance

**Data**
- Data segregation and isolation
- Information security and data privacy requirements
- Malicious insider

**Operational**
- Service reliability and uptime
- Disaster recovery
- SLA customization and enforcement
- Control over quality

**Technology**
- Evolving technology
- Cross-vendor compatibility and integration
- Customization limitations
- Technology choice and proprietary lock-in
Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Why auditing Cloud Computing on a periodic basis?</th>
<th>Data Protection</th>
<th>Technology Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To mitigate risks introduced by the Cloud</td>
<td>Assess following security methods and mechanisms:</td>
<td>Assess for the following:</td>
</tr>
<tr>
<td>• To evaluate efficiency of controls related to the Cloud</td>
<td>• Physical Security</td>
<td>• Server Virtualization patch management</td>
</tr>
<tr>
<td>• To continuously improve internal process, procedures and tools.</td>
<td>• Logical Security</td>
<td>• Super users</td>
</tr>
<tr>
<td></td>
<td>• Connection &amp; Data Transmission</td>
<td>• Segregation of duties</td>
</tr>
<tr>
<td></td>
<td>• Authentication &amp; Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Intrusion Detection &amp; Protection</td>
<td></td>
</tr>
</tbody>
</table>

Identity and Access Management

Assess efficiency and/or accuracy of:

• Approval Layers & Controls
• Granted access
• Removal of access rights
• Process for periodic review of access

Regulatory

Assess compliance with the following:

• Sarbanes Oxley compliance
• Privacy laws
• State Breach notification laws
• Regulatory requirements of other countries

Operations

Assess policies and procedures related to:

• Incident Management
• Problem Management
• Change Management
• Availability
Dimensions of Risk

Identity and Access Management

<table>
<thead>
<tr>
<th>Risk Dimension</th>
<th>Deployment Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and Access:</td>
<td>Private</td>
</tr>
<tr>
<td></td>
<td>Similar to traditional computing such as the following:</td>
</tr>
<tr>
<td></td>
<td>• Unauthorized access by current employees that no longer needs access</td>
</tr>
<tr>
<td></td>
<td>• Excessive number of individuals have access to applications that is not in accordance with ‘need-to-know’ basis of access rights management</td>
</tr>
<tr>
<td></td>
<td>• Use of shared accounts to administer the cloud applications and resources</td>
</tr>
<tr>
<td></td>
<td>Public</td>
</tr>
<tr>
<td></td>
<td>In addition to Private cloud computing risks, the following:</td>
</tr>
<tr>
<td></td>
<td>• For web-based applications, former employees might continue to retain access particularly if the identity and access management (IAM) for cloud, if there is one utilized for cloud applications, is not linked with the user’s on-premise IAM solution</td>
</tr>
</tbody>
</table>

Potential mitigation considerations

• Develop integrated identity and access management solution for applications hosted on private or public clouds that connect with existing/on-premise solution

• Periodic access reviews should include applications in the cloud
## Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Audit Objective(s)</th>
<th>Key Areas to Focus on during Audit</th>
</tr>
</thead>
</table>
| **Identity and Access Management:** Verify that only approved personnel are granted access to service based on their roles and that access is removed in a timely manner upon the personnel's termination of employment and/or change in their roles that does not require the said access. | - Physical Security  
- Hosting & Data Logical Security  
  - Segregation of tiers; hosting encryption methods  
  - Accessibility from the open Internet, over permissive rules that open wide range of ports  
- Authentication & Authorization  
  - Length / strength of passwords, systems to enforce / control password security / reset rules  
  - Use of hardware / software token. Management of key fobs  
- Only authorized users are granted access rights after proper approval  
- Access for transferred employees is modified in a timely manner  
- Unauthorized access to cloud computing resources is removed promptly  
- Periodic review of super-user and regular access to cloud applications  
- Connection & Data Transmission  
  - Secure connectivity such as VPN IPSec, SSL, HTTPS where secure data is being transmitted for regular users or administrators |

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International. 19259NJ
# Dimensions of Risk

## Data

<table>
<thead>
<tr>
<th>Risk Dimension</th>
<th>Deployment Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data:</strong></td>
<td></td>
</tr>
<tr>
<td>It is the risk associated with loss, leakage or unavailability of data. This can cause interruption to business, loss of revenue, loss of reputation, or even regulatory noncompliance in some cases.</td>
<td><strong>Private</strong></td>
</tr>
<tr>
<td><strong>Similar to traditional computing such as the following:</strong></td>
<td><strong>Public</strong></td>
</tr>
<tr>
<td>• Data leakage from malicious insider</td>
<td>• Unauthorized data access and/or modification by the service provider</td>
</tr>
<tr>
<td>• Lack of flexibility for segregation of duties</td>
<td>• Data co-mingling with other cloud tenants, particularly in case of SaaS</td>
</tr>
<tr>
<td></td>
<td>• Data leakage across shared infrastructure, particularly in case of IaaS</td>
</tr>
<tr>
<td></td>
<td>• Non-portability of data and metadata after termination of contract with cloud service provider</td>
</tr>
</tbody>
</table>

### Potential mitigation considerations

- Classify data and applications – include any encryption, co-location, and policy requirements as part of the classification scheme
- Access to data should be controlled in a manner consistent with your business and security requirements. For sensitive application and data, opt for dedicated capacity
- Consider options such as “data at home, application in the cloud”
### Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Audit Objective(s)</th>
<th>Key Areas to Focus on during Audit</th>
</tr>
</thead>
</table>
| **Data Protection:** Sufficiency of the data protection policies, procedures and practices at the Cloud Service providers as well as the user organization. | - Type and sensitivity of Data sent to and potentially stored in the cloud  
- Data protection requirements (business confidential information etc.)  
- Your (user) organization’s policies and procedures to protect data stored at third-parties  
- Co-mingling of your data with others tenants of the cloud application  
- Vendor’s overall capability maturity to meet the requirements  
- Understand the level of access (create/read/update/delete) that the vendor’s personnel have to the data, particularly for confidential information. For e.g. Microsoft has access to email content for the following: a) Operating and Troubleshooting the Services, and b) Security, Spam and Malware Prevention  
- If the vendor is unable to provide the right level of data protection, has your (user) organization put mitigating controls in place, such as removing sensitive data elements before sending it to the cloud or encrypting sensitive data  
- Understand the circumstances, if any, in which the vendor may disclose your data without your prior consent. Is that acceptable to your organization?  
- After potential termination of contract, portability of data and metadata (for e.g. format of the output/extract from the vendor) and purging of data by the service provider |
### Risk Dimension: Technology

Technology risk is associated with constantly evolving technologies and lack of standardization in how they integrate or interoperate. Technology risks could lead to costly re-architecture efforts for adoption or integration with new technology.

<table>
<thead>
<tr>
<th>Risk Dimension</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerging/evolving technologies present a lot of unknowns and takes time to mature. It will require re-tooling and retraining of employees</td>
<td>Limitations on customization of service offerings</td>
<td>Compatibility with other cloud providers</td>
</tr>
<tr>
<td>Limitations on customization of service offerings</td>
<td>Lack of technology choice</td>
<td></td>
</tr>
</tbody>
</table>

### Potential mitigation considerations

- Define a technology roadmap that standardizes the technologies used within an organization and supports decision on when to move to new technologies
- Maintain awareness – continually research and monitor developments by standards organizations, information security organizations (e.g. CSA), and technology vendors
- Standardize on integration methods such as web services API (most cloud providers use and/or support web services API) and ensure that data can be imported/exported in standard formats such as XML, CSV, etc.
Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Audit Objective(s)</th>
<th>Key Areas to Focus on during Audit</th>
</tr>
</thead>
</table>
| **Technology Risks:** Unique risks related to the use of virtual operating system with cotenants. | • Is your primary service provider utilizing another sub-service provider? For e.g. there are several examples where a SaaS provider is utilizing an IaaS provider. Do you know whether your primary service provider is protecting you adequately from the risks inherent with utilizing an IaaS provider?  
• Hypervisor technology utilized and whether it is patched  
• Process for monitoring and patching for known vulnerabilities in hypervisor technology  
• Segregation of duties (SoD) considerations both from a technology as well as business perspective, for e.g. from a technology SoD perspective does one person have access to the host and guest operating systems as well as the guest database. From a business perspective, for financially significant applications, just because an application is in the cloud does not diminish the importance of segregating access within the application  
• Logging of access to the applications and data, where relevant  
• Protection of access logs from inadvertent deletion or unauthorized access |
## Dimensions of Risk

### Operational

<table>
<thead>
<tr>
<th>Risk Dimension</th>
<th>Deployment Model</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational: Operational risk is associated with execution of business activities and services that rely on IT systems.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failover and availability concerns due to new and unproven technology</td>
<td>Connection response times and network bandwidth constraints, particularly if internet connection is used to access cloud</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of integration with existing service management tools and processes</td>
<td>Notification by the service provider of planned outages and status/resolution of unplanned outages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of Service Level Agreement (SLA) definition or enforcement with service provider</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduced control on application availability and disaster recovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Potential lack of service reliability and uptime due to prohibitive costs</td>
<td></td>
</tr>
</tbody>
</table>

### Potential mitigation considerations
- Prioritize applications and data that require High Availability
- Clearly define service level requirements and service level agreements with cloud service providers
- Establish availability and performance thresholds with service providers and request email alerts on threshold breaches
- Clearly define and mutually accept responsibilities between cloud service providers and client
# Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Audit Objective(s)</th>
<th>Key Areas to Focus on during Audit</th>
</tr>
</thead>
</table>
| **IT Support:**  | • Operational process documentation: policy, procedures, roles and responsibilities  
| Assess procedures related to incident management, problem management, change and access management in context of use of Cloud services. | • Effectiveness of Service Level Agreement (SLA) monitoring  
| | • Appropriate use of monitoring tools and reports  
| | • Communication protocol/who at your (user) organization is notified by the vendor during scheduled outage windows and non-scheduled outages  
| | • In case of SaaS, coordination of release schedule and sign-off/approval for change management and testing of new functionality within the application  
| | • Does your organization (user) have a periodic backup of data at the cloud service provider, particularly in case of SaaS  
| | • Assignment of responsibility at the user organization for periodic review of Availability and performance reports provided by the service provider |
### Dimensions of Risk

#### Regulatory

<table>
<thead>
<tr>
<th>Risk Dimension</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory: Regulatory risk is associated with noncompliance to various legal, government, and regulatory requirements.</td>
<td>Similar to traditional computing</td>
<td>Lack of visibility into cloud operations and ability to monitor for compliance with regulations such as State-level privacy breach notification laws and HIPAA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of monitoring and notification to user organization of breach in confidentiality of information in the cloud leading to regulatory sanctions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dependence on service provider to help ensure adequate internal controls</td>
</tr>
</tbody>
</table>

#### Potential mitigation considerations

- Work closely with internal audit, risk, and security organizations from the start of any cloud computing
- Ask cloud service providers for relevant certifications such as SOC reports, ISO 27001 certification, etc. Reserve the “right to audit” the cloud service providers
- Monitor developing regulations and standards as they mature to proactive assess their impact of your cloud-based operations
## Auditing Cloud Computing in Five Relevant Areas

<table>
<thead>
<tr>
<th>Audit Objective(s)</th>
<th>Key Areas to Focus on during Audit</th>
</tr>
</thead>
</table>
| **Regulatory:** Compliance with regulatory requirements over the protection of information | - Regulatory requirements, such as Sarbanes Oxley Act (controls over initiation, authorization, processing and recording of transactions) or privacy, such as Health Insurance Portability and Accountability Act (HIPAA) or State Privacy Breach notification laws  
- Intrusion Detection & Protection practices at the cloud service provider  
- Does the vendor know whom to notify when a breach happens? For e.g. from Microsoft's Office365 website¹: “Our notice will typically be delivered by email to one or more of the administrator(s) the customer has listed in the online services portal. It is the customer’s responsibility to ensure contact information remains up to date.” Do you want important legal notices served to your system administrators?  
### Sample Approach for Auditing Cloud Service Providers

#### Prep
- Develop Audit Plan, Control Objectives and Review Steps
- Interview IT and business leaders to understand company's position / vision of Cloud
- Select relevant Cloud services / projects as audit samples

#### Fieldwork
- Gather documentation and evidence via DRLs in regards to Audit Objectives
- Interview Stakeholders and Analysts
- Perform Tests of Design and Operational Effectiveness against Audit Review Steps

#### Findings
- Document gaps with Controls Objectives and related risks
- Provide recommendations to address issues identified during audit
Common Observations When Auditing Cloud Computing

- Password settings for cloud resources (applications, virtual servers etc.) does not comply with user organization’s password policies. Sometimes the cloud vendor resources do not support the user organization’s policy requirements, but several times, the cloud administrators at the user organizations are not aware.
- Port settings on Cloud server instances not appropriately configured (administrator added exceptions to administer cloud from their home computer and mobile device).
- Lack of policy and procedures for appropriate handling of security and privacy incidents.
- Terminated users found to be active on applications in the cloud (even though the individual’s network access was terminated) and there was no IP range restriction.
- Employees transferred out of a certain department had access to Cloud resources even though they transferred to another department a few months ago.
- Service provider’s SOC report was not reviewed for impact to user organization.
- Sensitive data (PII) in the cloud was found to be not encrypted. Sometimes the user organization is not aware that sensitive data resides in the cloud. Most commonly, with the use of cloud for test environments, sensitive data is not scrambled/de-identified before being sent to the cloud. It might even be your third-party development vendor doing that.
- Use of shared accounts to administer the cloud.
Good Practices in Cloud Computing

• Sensitive data (PII) is encrypted before sending to the cloud
• Making sure that multiple people receive notifications from the cloud service provider and that list of individuals/email id is periodically reviewed and updated. This is simple to implement and very beneficial
• Several cloud service providers offer the option of IP range restriction. That could be a great tool in utilizing a cloud-based services but having the security comfort of in-house IT
• Use of secure connection when connecting to the cloud, anytime sensitive data is exchanged
• Access to cloud computing resources is integrated with the user organization’s identity and access management process instead of being handled one-off
• Use of multi-factor authentication (MFA) such as hardware/software tokens, mobile authentication (particularly if the mobile phone is a company resource) for administration of cloud resources. This could also protect in case the user organization’s employees are subject to phishing attack
• Review proper independent review report/certification: sometimes a SOC report is not sufficient
What do you think?
Share your thoughts about this presentation on Twitter using the hashtag #IIACHI

Follow us on Twitter
@IIAChicago

Not on Twitter?
Visit our Social Media booth in the Exhibit Hall to join the conversation today!