Cloud IT, Privacy, and Security

June 13, 2013
Chris Kradjan, CPA, CITP, CRISC

Chris Kradjan is the National Leader for IT Consulting and the SSAE 16 Practice of Moss Adams. With more than 16 years of experience, he serves a variety of complex technology-based service organizations. His practice areas include SSAE 16 auditing, internal controls reviews, Sarbanes-Oxley compliance services, PCI-DSS services, SysTrust/WebTrust audits, and independent technology assessments. Chris is responsible for quality assurance involving IT audits performed by Moss Adams. Chris has developed and continues to maintain oversight of the firm's SSAE 16 audit and technology review compliance practices.
Agenda

• Define “cloud computing” terms
• Outline risks and benefits
• Talk about challenges of compliance in the cloud
• Consider issues from provider and consumer perspective
• Best practices for success
• Questions
Administrative Systems

- Resident billing
- Medical billing
- Fundraising
- Grants management
- Data warehouse
- Financial accounting
- HR and time entry
- Office automation
- Internet
- Remote access
Infrastructure

• Distributed network environment
• Many wireless access points
• Complexities with licensing compliance
• Security and other practices can vary by site
• Can be challenges in older facilities
• May involve multiple providers
Systems for Residents

- Kiosks
- Point of sale
- Dining
- Facilities
- Resident billing
- Clinical and EMR
- Tablets/BYOD
- Internet access
- Safety, health and wellness
- Social interaction
Resident Care

- Wireless point of care systems
- Personal health records
- Remote monitoring
- Fall detectors
- First alert responders
- Motion sensors in living space
- Telehealth monitoring
- Caregiver network accessibility
- Videoconferencing
- Cognitive fitness
Cloud Computing

Cloud Computing

Having secure access to all your applications and data from any network device

Cloud Computing Visual Diagram from Wikipedia on Cloud Computing
Haze of Terminology

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Public, private, hybrid and community clouds
- Application Service Provider (ASP)
- Third-party hosting
- Co-locations
- Vendor managed solution
Question #1

How would you classify your organization?

1. SaaS cloud provider
2. PaaS cloud provider
3. IaaS cloud provider
4. Current consumer of the cloud
5. Planned consumer of the cloud
6. Still learning about the cloud
Cloud Computing Visual Model

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Essential Characteristics

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Service Models

- Public
- Private
- Hybrid
- Community

Deployment Models

Cloud Security Alliance from the “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1” pg.14
<table>
<thead>
<tr>
<th>Cloud Deployment Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Cloud (External)</strong></td>
<td>The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.</td>
</tr>
<tr>
<td><strong>Private Cloud (Internal)</strong></td>
<td>The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.</td>
</tr>
<tr>
<td><strong>Hybrid Cloud (Mixed)</strong></td>
<td>The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.</td>
</tr>
<tr>
<td><strong>Community Cloud (Shared)</strong></td>
<td>Shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.</td>
</tr>
</tbody>
</table>

*Cloud Security Alliance from the “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1” pg.17*
## Essential Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-Demand Self-Service</strong></td>
<td>The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service’s provider.</td>
</tr>
<tr>
<td><strong>Broad Network Access</strong></td>
<td>According to NIST, the cloud network should be accessible anywhere, by almost any device (e.g., smart phone, laptop, mobile devices, PDA).</td>
</tr>
<tr>
<td><strong>Resource Pooling</strong></td>
<td>The provider’s computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.</td>
</tr>
<tr>
<td><strong>Rapid Elasticity</strong></td>
<td>Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.</td>
</tr>
<tr>
<td><strong>Measured Service</strong></td>
<td>Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.</td>
</tr>
</tbody>
</table>
## Key Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offsite</td>
<td>IT resources are accessed from an offsite data center that is not owned by you; thus yielding savings in cost of ownership, licenses etc.</td>
</tr>
<tr>
<td>Virtual</td>
<td>Software stacks of databases, web servers, operating systems, storage, and networking are assembled virtually and accessed via the web</td>
</tr>
<tr>
<td>On-Demand</td>
<td>Use as needed, resources can be turned on or off quickly and as needed including storage capacity, databases, web servers and operating systems</td>
</tr>
<tr>
<td>Pay-Per-Use</td>
<td>Pay for what you need, not for unneeded capacity</td>
</tr>
<tr>
<td>Simple</td>
<td>Resources can be configured quickly and easily, e.g. leading cloud computing platforms have open API’s</td>
</tr>
<tr>
<td>Massive Scale</td>
<td>Access to extremely large infrastructure that would be challenging to build as a single entity</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>The use of cloud computing for storage capacity can be ideal, especially for spikes in usage. Because the use of the cloud entails low or no upfront capital costs and low ongoing operational costs, the ability to take advantage of pools of resources on demand in real-time can yield business advantage</td>
</tr>
<tr>
<td>Elasticity and Resizability</td>
<td>Ability to be highly flexible – nearly instantaneously – to changes in load. With cloud computing, an infrastructure supporting an application, business, or business process can be easily resized and right-sized, depending upon conditions</td>
</tr>
<tr>
<td>Collaboration</td>
<td>Shared environment, IT resources can be consolidated, many users share a common network, allowing costs to be managed</td>
</tr>
</tbody>
</table>

*AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?*
Cloud Drivers

- On demand storage, CPU, and servers
- Hardware failure and upgrades eliminated
- Gain flexibility and speed in implementations
- Scalability – Quickly provision capacity as needs change
- Sustainability
- Availability zones for disaster recovery
- Leverage IT technology evolution
- Professional infrastructure management
Benefits of Cloud Computing

- Cost containment
- Immediacy
- Availability
- Scalability
- Efficiency
- Resiliency
Allure of Cost Savings

- Economies of scale
- Reduced capital to build IT capability
- Manageable monthly costs
Another Perspective

More than 75% of the IT budget today is spent on maintaining and running existing systems and software infrastructure – Gartner Group
Question #2

What would you consider your primary driver for going to the cloud?

1. Cost containment
2. Immediacy
3. Availability
4. Scalability
5. Efficiency
6. Resiliency
Cloud Leaders

- Amazon Web Services
- Cisco Systems
- Google
- IBM
- Microsoft
- Oracle
Market Direction

• U.S. powerhouses
• Multi-national footprint
• Massive leverage
• Centralized consumer data
• Powerful data analytics
Case Study: Amazon

- **IAAS**
  - Amazon Elastic Compute Cloud (EC2)
  - Amazon Elastic MapReduce
  - Amazon Virtual Private Cloud (Amazon VPC)
  - Amazon Route 53

- **PAAS**
  - Amazon DynamoDB
  - Amazon Relational Database Service (RDS)

- **SAAS**
  - Does not provide SAAS solutions
  - Other SAAS providers can leverage IAAS and PAAS players like Amazon to move into the cloud
IAAS and PAAS

- Align with the major players
- Determine service offerings
- Establish tiers of clients
- Define service levels by tier
- Link usage to revenue
- Institute metrics
- Implement tools to efficiently track usage
- Architect for security and privacy protections
- Institutionalize controls and compliance functions
SAAS

- Migrate existing solutions to the cloud
- Partner with IAAS and PAAS providers
- Find smartphone and internet applications
- Establish external facing connections
- Embed analytical capabilities
- Adopt similar service levels, metrics, revenue models and control measures as IAAS and PAAS
Common Cloud Services

- Financial accounting system  (*Intacct, NetSuite*)
- Email   (*Apptix, Avanade, Go Daddy, Microsoft Hosting*)
- Office automation and calendaring   (*Google Docs, Office 365*)
- CRM   (*Salesforce*)
- Backup   (*Barracuda, CrashPlan, Mozy, Symantec, Symform*)
- Data analytics   (*CCI, ECI, MedeAnalytics, PivotLink*)
- Storage   (*Amazon Web Services (AWS), DropBox, Google Cloud Storage, JustCloud.com, Microsoft Azure, SkyDrive*)
- Virtual machine environments
- Operating systems, database platforms and test environments   (*AWS, Amazon EC2, Azure, Google App Engine, Google Compute Engine*)
- Colocation facilities
Consumers

- Understand your IT portfolio and service needs
- Evaluate options in the market
- Determine which cloud deployment model(s) are a fit
- Define a cloud strategy
- At a minimum, look where private clouds are viable
- Require SLAs
- Assess the costs factors
- Build in rate increase limits
- Look at full lifecycle of data management
- Be mindful of transition and/or exit strategy if a provider ceases to operate
Question #3

What are the greatest challenges you see with the cloud?

1. Security
2. Privacy
3. Loss of control
4. Inherent limits to the services offered
5. Risk of the unknown
6. Other
Negative Perceptions

- Loss of control
- Hidden costs – renewal rates rise, obscure cost provisions, etc.
- Integration costs and vendor lock-in
- Service reliability (emerging vendors)
- Physical location of data storage (crossing state and national borders, with varying privacy laws)
- Unclear who owns rights to the data
- Inability to customize
- Infrastructure limitations
- Brand management
### Risks, Threats & Vulnerabilities

<table>
<thead>
<tr>
<th>Availability</th>
<th>Service availability and recoverability, complexity, single-points-of-failure, data replication, testing constraints, and over-subscription risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Multi-tenancy, data access, and secure data deletion</td>
</tr>
<tr>
<td>Authentication</td>
<td>External authentication, federated authentication, key management, cloud to cloud authentication</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Audit rights and compliance</td>
</tr>
<tr>
<td>Integrity</td>
<td>Shared environments, data monitoring, and data encryption</td>
</tr>
<tr>
<td>Privacy</td>
<td>Legal uncertainties, individual rights/confidentiality, and breach/disclosures</td>
</tr>
<tr>
<td>Operational Security</td>
<td>Vulnerability management, asset management, and incident response</td>
</tr>
</tbody>
</table>

*Source: AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?*
<table>
<thead>
<tr>
<th>Security Category</th>
<th>Risks, Threats &amp; Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td><strong>Service Availability and Recoverability</strong></td>
</tr>
<tr>
<td></td>
<td>• Cloud provider may not be able to match in-house IT service availability, recovery time objectives (RTO), and recovery point objectives (RPO)</td>
</tr>
<tr>
<td></td>
<td>• Cloud providers may drastically change business model or discontinue cloud services</td>
</tr>
<tr>
<td><strong>Complexity</strong></td>
<td>• Complexity introduced by cloud computing environment results in more pieces that can go wrong, and more complex recovery procedures</td>
</tr>
<tr>
<td><strong>Single-Points-of-Failure</strong></td>
<td>• Even if the cloud environment is architecturally designed for high-availability, single-points-of-failure may exist in the access path to the cloud</td>
</tr>
<tr>
<td><strong>Data Replication</strong></td>
<td>• Due to technical architecture complexity and potentially restrictions by the cloud provider, replicating data back to the enterprise or to another provider may be difficult</td>
</tr>
<tr>
<td><strong>Testing Constraints</strong></td>
<td>• Due to concerns about confidentiality and impact to other customers, cloud providers may place heavy constraints on disaster recovery testing activities</td>
</tr>
<tr>
<td><strong>Over-Subscription Risk</strong></td>
<td>• In the event of a disaster, other customers may receive higher priority in recovery activities</td>
</tr>
<tr>
<td></td>
<td>• As cloud providers shift from investment mode to capture market share to cost cutting mode to reach profitability, capacity may become constrained</td>
</tr>
</tbody>
</table>
### Risks, Threats, Vulnerabilities (2/6)

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Risks, Threats &amp; Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Multi-Tenancy</strong></td>
<td>• Data is possibly exposed to 3rd parties due to lack of access controls on the cloud, allowing unauthenticated parties access to confidential data</td>
</tr>
<tr>
<td><strong>Data Access</strong></td>
<td>• Cloud stores data without proper customer segregation allowing possible disclosure to 3rd parties</td>
</tr>
<tr>
<td><strong>Secure Data Deletion</strong></td>
<td>• Company data that was deleted is still be retained on servers or storage located on the cloud without knowing</td>
</tr>
</tbody>
</table>

*AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?*
<table>
<thead>
<tr>
<th>Security Category</th>
<th>Risks, Threats &amp; Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td><strong>External Authentication</strong></td>
<td>Ownership and maintenance of credential repositories is the responsibility of an external party. Security leading practices cannot be guaranteed</td>
</tr>
<tr>
<td><strong>Federated Authentication</strong></td>
<td>Organizations implement single sign on applications used by multiple business partners but the SSO also grants access to sensitive internal information due to authentication mashups</td>
</tr>
<tr>
<td><strong>Key Management</strong></td>
<td>Any activity related to key generation, exchange, storage, safeguarding, use, vetting, and replacement that results in disclosure will provide access to infrastructure and data</td>
</tr>
<tr>
<td><strong>Cloud to Cloud Authentication</strong></td>
<td>One cloud provider will rely on a second cloud provider to authenticate a user’s identity based on the first cloud passing a SAML assertion to the second cloud at the request of a user. Based strictly on the assertion, the second cloud provider will grant the user access to cloud resources. SAML assertions are susceptible to the following attacks: DoS, Man-in-the-Middle, Replay, and Session Hijacking</td>
</tr>
</tbody>
</table>

*AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?*
## Risks, Threats, Vulnerabilities (4/6)

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Risks, Threats &amp; Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulatory</strong></td>
<td><strong>Audit Rights</strong></td>
</tr>
<tr>
<td></td>
<td>• Organizational Rights to perform audits, and review performance against contracts or SLA</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Migration to the cloud includes a more complex regulatory environment for some corporations</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td><strong>Shared Environments</strong></td>
</tr>
<tr>
<td></td>
<td>• Data in cloud is in a shared environment alongside data from other customers</td>
</tr>
<tr>
<td><strong>Data Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Changes made to data without knowledge of the data owners, or accidental overwrites due to collisions with data storage techniques of cloud provider</td>
</tr>
<tr>
<td><strong>Data Encryption</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data at rest is not encrypted and accessed by 3rd parties unknowingly due to faulty access controls</td>
</tr>
</tbody>
</table>

*AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?*
### Risks, Threats, Vulnerabilities (5/6)

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Risks, Threats &amp; Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td><strong>Legal Uncertainties</strong>&lt;br&gt;• Multiple jurisdictions increase regulatory complexity&lt;br&gt;• Conflicting legal provisions create significant uncertainty in assessing compliance and risk&lt;br&gt;• The Privacy and Data Protection legal landscape continues to evolve at a rapid pace&lt;br&gt;• Data sharing agreements may be required before moving data to the cloud&lt;br&gt;  – Business associate agreements (HIPAA)&lt;br&gt;  – Data controllers and third parties (EU DPD)</td>
</tr>
<tr>
<td></td>
<td><strong>Individual Rights/Confidentiality</strong>&lt;br&gt;• Strict terms of service are particularly important in the cloud to preserve individual privacy/confidentiality and to meet regulatory requirements to which the user is subject&lt;br&gt;• The cloud facilitates the ability to use/share data across organizations and therefore increase secondary uses of data that may require additional consent/authorization&lt;br&gt;• Data is easily accessible by a larger group of users and must be strictly controlled (Protect data at rest)</td>
</tr>
<tr>
<td></td>
<td><strong>Breach/Disclosure</strong>&lt;br&gt;• Centralized data stores are especially prone to security breaches&lt;br&gt;• Timely discovery and reporting of the breach by the cloud provider may be challenging</td>
</tr>
</tbody>
</table>

_AICPA Webinar Cloud Computing Security and Governance - What Auditors Need to Know?_
## Security Category

### Operational Security

**Vulnerability Management**
- One vulnerability has the potential to expose large number of corporations critical assets

### Asset Management
- Assets in the cloud are not properly managed and could leak critical company information or cause data exposures

### Incident Response
- Ownership, responsibilities, and actions during incident response are not defined
A recent survey was conducted of IT executives/CIOs about their companies’ use of, and views about, IT cloud services.

The biggest cloud challenge reported was security.
Regulators Perspective

- Personally Identifiable Information
  - Federal requirements – NIST 800-53
  - State data breach and privacy laws
  - Healthcare and patient data: HIPAA Security Rule
  - FERPA compliance
  - Safe Harbor
- Internal Controls over Financial Reporting:
  - SOC/SSAE 16 audits (previously SAS 70 audits)
  - Sarbanes-Oxley
- ISO 27002
- Payment Card Data: PCI-DSS
  - QSA audit of service provider
- Document retention, e-discovery, and public records
  - Retention policies and practices
Cloud Security Alliance

Cloud Controls Matrix

- Compliance
- Data Governance
- Facility Security
- Human Resources
- Information Security
- Legal
- Operations Management
- Risk Management
- Release Management
- Resiliency
- Security Architecture
Making the Business Case

Have a clear and upfront understanding of:

• Decision drivers to enter the cloud
• Current state of your IT
• True costs
• Economies of scale
• Integration needs
• Risk

NACUBO Whitepaper: Capturing the Cloud, Defining the Business Case (http://www.nacubo.org)
Question #4

When do you see your organization making the move to the cloud?

1. Already in the cloud
2. Over the next year
3. In the next 2 to 3 years
4. More than 3 years out
5. Never
Making the Business Case

Have a clear and upfront understanding of:

- Decision drivers to enter the cloud
- Current state of your IT
- True costs
- Economies of scale
- Integration needs
- Risk

NACUBO Whitepaper: Capturing the Cloud, Defining the Business Case (http://www.nacubo.org)
Proper Preparation

• Embrace the cloud, but only where it makes sense
• Have an organization-wide solution
• Define requirements
• Perform proper due diligence
• Select good vendors with solid track records
• Review contracts carefully
• Have an exit strategy
• Own the implementation and the system use
• Monitor vendor performance and outcomes
• Enforce client controls
• Consider regulatory compliance
Summary

• Cloud computing is an increasing trend
• Significant benefits will drive adoption, despite the concerns
• Avoid the hype and focus on where it has value for you
• Institute solutions with sufficient demand and market scale
• Focus on vendor selection, management, and due diligence
• Know and manage the risks
• Do not transfer all control responsibility
Questions

Chris Kradjan, CPA, CITP, CRISC
Partner, National IT Practice Leader
(206) 302-6511 / (415) 677-8343
chris.kradjan@mossadams.com