AUDITING THE CLOUD ENVIRONMENT

ISACA New England Annual General Meeting

June 2019
AGENDA

03 Cloud Models Overview
   What Are We Hearing From Our Clients?
   Multiple Models of Cloud Computing
   Cloud Computing Deployment Models
   Visibility Into Cloud Risks

08 Cloud Auditing Areas of Focus
   Standards for Managing Cloud Risks
   Cloud Computing Audits/Projects
   Cloud Business Considerations
   Cloud IT Auditing Focus Areas
CLOUD MODELS OVERVIEW
WHAT ARE WE HEARING FROM OUR CLIENTS?

Management’s understanding of the cloud is limited.

The pros and cons of using a cloud environment are not always weighed effectively.

Cloud auditing methods are not always considered when choosing a cloud vendor or developing a cloud strategy.

The Third Party Risk Management portion of cloud auditing is often overlooked.

Cloud computing audits are often re-scoped, as companies underestimate (or overestimate) the maturity of their cloud environment.
MULTIPLE MODELS OF CLOUD COMPUTING

Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction OR simply, IT runs over the internet instead of installing hardware and software yourself.

**Characteristics**
- On demand self-service
- Pay as you use (measure service)
- Rapid elasticity (expand/contract)
- Multi tenancy (shared pool)
- Broad network access

**Service Models**
- **Software as a Service (SaaS)**
  Finished applications that you license on a subscription basis, sometimes customizable
- **Platform as a Service (PaaS)**
  Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity
- **Infrastructure as a Service (IaaS)**
  Deployment platform that abstracts the infrastructure

**Deployment Models**
- Public Cloud
- Hybrid Cloud
- Private Cloud
CLOUD COMPUTING DEPLOYMENT MODELS

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Cloud</strong></td>
<td>It is also known as internal cloud or on-premise cloud, a private cloud provides a <strong>limited access to its resources and services</strong> to consumers that belong to the same organization that owns the cloud.</td>
</tr>
</tbody>
</table>

| **Public Cloud** | It is also known as external cloud or multitenant cloud. It is **available and open used by general public.** |

| **Hybrid Cloud** | It is **composition of two or more distinct cloud infrastructure (private or public)** but are bound together by standardized technology that enable data and application portability. (Ex: AWS VPC, DirectConnect) |

Source: [IJARCSSE- An Overview of Cloud Computing](#)
## ADVANTAGES AND DISADVANTAGES

<table>
<thead>
<tr>
<th>Model</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| **SaaS** | • Most cost effective cloud service, leasing the software only and not a resource  
• Minimal planning required and easy setup  
• Rapid deployment and scalability  
• Provider is responsible for application management | • Customer has no control over the system processing their data  
• No control over who uses the software  
• Little control over application upgrade and features  
• Provider has full access to customer’s data  
• Integration with legacy applications can be difficult |
| **PaaS** | • Somewhat cost effective, leasing a software platform and not a resource  
• Customer can bring their own software onto PaaS  
• Customer has level of control over users accessing software  
• Minimal management of the VM by the customer  
• Ability to use APIs (application programming interface), applications can "talk" with each other on the cloud stack | • Lack of control over the VM or processing of data, can present security risk over data  
• Platform most likely shared and used by other customers running their applications  
• Can be difficult to integrate PaaS services with legacy applications and systems |
| **IaaS** | • Customer has full control of VM and everything inside it  
• Integration with enterprise infrastructure is simplified  
• Potentially most secure Cloud service  
• Customer run and control their own virtual interface without the cost and maintenance of hardware  
• Elimination of data center hardware | • The most expensive of the services, customer is leasing a tangible resource  
• Customer is responsible for back ups  
• Customer is responsible for all VM management  
• No control over which server the cloud provider stores their data or the geographical location of the server |
SHARED RESPONSIBILITY MODEL
VISIBILITY INTO CLOUD RISKS

As visibility is lost…
• Where is the data?
• Who can see the data?
• Who has seen the data?
• Has data been tampered with?
• Where is processing performed?
• How is processing configured?
• Is use of processing resources monitored?
• Does backup happen? How? Where?

… security, compliance, and value can be lost well.
CLOUD AUDITING AREAS OF FOCUS
AUDITS/PROJECTS AROUND CLOUD COMPUTING

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud computing platform evaluation/due diligence</td>
<td></td>
</tr>
<tr>
<td>Data migration review to the new platform</td>
<td></td>
</tr>
<tr>
<td>Management of the cloud computing function</td>
<td></td>
</tr>
<tr>
<td>Security reviews</td>
<td></td>
</tr>
<tr>
<td>• Security of data</td>
<td></td>
</tr>
<tr>
<td>• Network accessibility</td>
<td></td>
</tr>
<tr>
<td>• User administration</td>
<td></td>
</tr>
<tr>
<td>Regular review of SOC Type 1/provider sponsored audit reports</td>
<td></td>
</tr>
<tr>
<td>Cost/Savings impact</td>
<td></td>
</tr>
<tr>
<td>Realignment of controls for regulatory reporting</td>
<td></td>
</tr>
<tr>
<td>SLA/KPI review to ensure the provider is living up to their end of the bargain</td>
<td></td>
</tr>
<tr>
<td>Impacts to Disaster Recovery/Business Continuity</td>
<td></td>
</tr>
</tbody>
</table>
STANDARDS FOR MANAGING CLOUD RISKS

COBIT

The Control Objectives for Information and Related Technology (COBIT) released by IT Governance Institute and the Information Systems Audit and Control Association (ISACA) focuses on developing, implementing, monitoring and improving IT governance and management practices. Past versions focused on auditing, but more recently the emphasis has moved toward information governance to provide more guidance on control and security in the cloud as those services become more prevalent.

CSA

The Cloud Controls Matrix (CCM) designed by the Cloud Security Alliance (CSA) provides guidance to cloud vendors and prospective customers on how best to assess security risk and gives organizations details on information security specific to their industries. It emphasizes business information security control requirements; reduces and identifies consistent threats and vulnerabilities in the cloud; provides standardized security and operational risk management; and seeks to normalize security expectations, cloud taxonomy and terminology, and security implemented in the cloud.

NIST

The National Institute of Standards and Technology (NIST) Cybersecurity Framework was created by collaborating with the government and private sectors to address and manage risk based on business needs without additional regulatory requirements. It assembles standards, guidelines, and practices that are already working effectively and can be used as a model by companies overseas to strengthen international cybersecurity.
When the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed, it was intended to protect patients’ physical medical records and the diffusion of their information. Now, widespread adoption of cloud services has expanded HIPAA’s reach and reaffirmed the importance of cloud security, especially in healthcare. HIPAA is now careful to regulate who can edit and access patient information in the cloud.

The Payment Card Industry (PCI) Security Standards Council promotes safety of cardholder data around the world by working with all entities associated with payment cards. The main objectives are to assist merchants and financial institutions implement security policies, technologies, and processes that protect their systems from breaches and theft of cardholder data, as well as to help vendors develop secure payment solutions. This has become more important as more transactions occur online and cardholder data is stored in the cloud, rather than solely in physical form.
CLOUD BUSINESS CONSIDERATIONS

HOW DO ORGANIZATIONS MEASURE THE POTENTIAL COST SAVINGS?

The business model must have sufficient detail to estimate cost in terms which can be applied to the cloud provider’s cost model. For infrastructure as a service (IaaS) and platform as a service (PaaS), this might be measured in resource usage per period of time, as for processing, throughput and storage. For software as a service (SaaS), service might be measured by number of transactions or number of users. Variables to consider:

- User characteristics, e.g. user types/roles, number of users, usage scenarios;
- Data characteristics, e.g. data types, size and quantity;
- Average usage rates, e.g. transactions per second
- How usage rates will vary, e.g. upper and lower ranges;
- Where can changes to usage rates be predicted, either at planned times or based on events;
- How usage will grow or scale over time, perhaps with the number of users; and
- How usage will change for each system actor, e.g. end user, administrator, batch processes.

WHAT ARE THE BUSINESSES REQUIREMENTS?

For each requirement, determine which are mandatory and which are desirable. Consider leveraging a standard practice description, such as the IT Infrastructure Library (ITIL), to ensure coverage of requirements which relate to the management of services.
Areas necessary to evaluate when auditing the cloud:

- Business Continuity
- Incident Management
- Governance
- Vendor Management
- Availability
- Data Security
CLOUD IT AUDITING AREAS OF FOCUS (2/8)

Governance

Key Questions

- What is the organization’s strategy around cloud technologies?
- Are there policies and procedures in place defining cloud governance requirements and processes?

Common Controls

- Cloud Governance policies and procedures are documented, reviewed annually, and contain the following:
  - Data classification and acceptable use practices
  - Administrative policies
  - User roles and responsibilities, access permissions and associated personnel appropriateness
  - Access provisioning and de-provisioning processes
- The Company ensures that customer, IT information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the organization.
CLOUD IT AUDITING AREAS OF FOCUS (3/8)

Vendor Management

- How does the organization manage vendor relationships to mitigate third party risk?
- Are appropriate controls in place over contract considerations and relationship management?
- How does the organization ensure appropriate controls are in place at cloud vendors to protect confidential data?
- Are appropriate controls in place at the organization to review vendor attestation reports and map user controls considerations?

Key Questions

- Relationships between the Company and third party vendors are managed by an appointed Vendor Relationship Manager, including regular meetings/touchpoints with client representatives.
- Contracts exist between the Company and third party vendors and ensure the following are appropriately defined:
  - Data Ownership, Retention, and Legal Hold
  - Data Segregation
  - Data Location & Servicing
  - Legal Compliance
  - End of Service Provisions and Data Delivery
  - Right to Audit
Vendor Management Cont’d

- The Company reviews attestation reports of third party vendors to ensure the report scope is relevant to the Company and the following areas are defined:
  - Physical security and environmental controls to protect confidential data
  - Incident monitoring processes are implemented and actively used by the service provider to document and report all defined incidents
  - Data backup and data storage controls
  - Logical access controls to applications and servers containing organization data
- The Company identifies the relevant User Controls Considerations in attestation reports and ensures controls are in place at the Company to mitigate any additional risk.
- The Company reviews attestation reports for any noted exceptions, Management evaluates the impact and risk as it pertains to Company’s environment, and follows up with the vendor as necessary.
Availability

• How is cloud vendor performance monitored and measured?

• How does the organization ensure Service Level Agreements meet the organizations needs and agreed upon service levels are being met?

Common Controls

• Service Level Agreements are in place and define service level benchmarks for all third party vendors.

• Management calculates service levels to ensure requirements of the Service Level Agreement are being met. Management periodically reviews third party vendor Service Level Agreements to ensure the organization’s needs are being met.

• Key Performance Indicators ("KPI") are defined for third party vendors in respective agreements. Agreements define incentives and penalties for achieved and missed KPIs, and are enforced as applicable.

• Management assigns appropriate personnel to monitor utilization and capacity of third party vendor services.
CLOUD IT AUDITING AREAS OF FOCUS (6/8)

Data Security

Key Questions

- Are appropriate security and access controls in place over cloud technologies?
- What monitoring is performed over user provisioning?
- How does the organization ensure duties are segregated appropriately?
- How is data encrypted, during transit and at rest?
- How is administrator access provided and monitored?

Common Controls

- Users are provisioned access to applications upon approval by appropriate personnel.
- Upon employee termination or department transfer, access is removed or modified to meet the responsibilities of their new status in a timely manner.
- Users are required to authenticate to applications with a unique user ID and password. Passwords are required to meet complexity requirements as stated in the Password Policy.
- User profiles are reviewed on a periodic basis to validate access is appropriately restricted and aligned with the user's functional responsibilities.
- Data loss prevention is implemented in the system and monitors all outgoing traffic to cloud service providers. Files containing sensitive data that violate policy are quarantined and must be released by appropriate personnel.
- Policies and procedures for data encryption are documented and periodically reviewed by Management. Data at rest is encrypted and data in transit is encrypted over networks.
CLOUD IT AUDITING AREAS OF FOCUS (7/8)

Business Continuity

Key Questions

• What is the organization’s strategy to ensure operations will continue in the event a cloud vendor can no longer provide a service?

• How often are business continuity plans tested?

Common Controls

• Procedures, capabilities and alternatives are established, maintained and tested, and a state of readiness has been established to transfer cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations.

• Redundancy plans for third party vendors are reviewed on an annual basis and modified as necessary.

• Company business continuity and disaster recovery plans are defined and tested at least annually.
CLOUD IT AUDITING AREAS OF FOCUS (8/8)

Incident Management

Key Questions

- How does the organization ensure the appropriate controls are in place to notify third party vendors of security incidents?
- How is the organization notified of vendor incidents that may affect the organization’s data?
- What are the service level and operating level agreements (SLAs and OLAs)?

Common Controls

- The contract/service agreement describes specific definitions of incidents (data breaches, security violations) and events (suspicious activities) and the actions to be initiated by and the responsibilities of both parties.
- Business should be involved in drafting legal, regulatory or contractual compliance requirements.
- Specific requirements to consider include:
  - Availability metrics include a unit of time, e.g. downtime per month;
  - Guaranteed maximum outages and outage durations if reliability is critical;
  - How much data can be lost and the minimum acceptable time to recover from both transient and catastrophic failures;
  - Both average and peak response times for various types of transactions; and
  - The data size for transactions, and peaks and averages from the usage model.
  - How to report incidents to cloud vendors
  - How the vendor will notify the organization that an incident occurred
  - The roles and responsibilities of the Company and the vendor when an incident occurs
QUESTIONS?
CONTACT INFORMATION

Matthew Levine
Associate Director, IAFA – IT Audit
matthew.levine@protiviti.com

125 High Street, 17th Floor
Boston, MA 02110
Office: +1 617-646-2709