



cutting through complexity™

Cloud Computing – An Internal Audit Perspective

Heather Paquette, Partner

Tom Humbert, Manager

March 10 2011

Discussion Agenda

- Introduction to cloud computing
- Types of cloud services
- Benefits, challenges, and risks
- Questions for auditors
- Emerging good practices
- User auditor assurance and Other approaches
- Risk-based Audit Scoping Utilizing RiskIT and COBIT
- 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

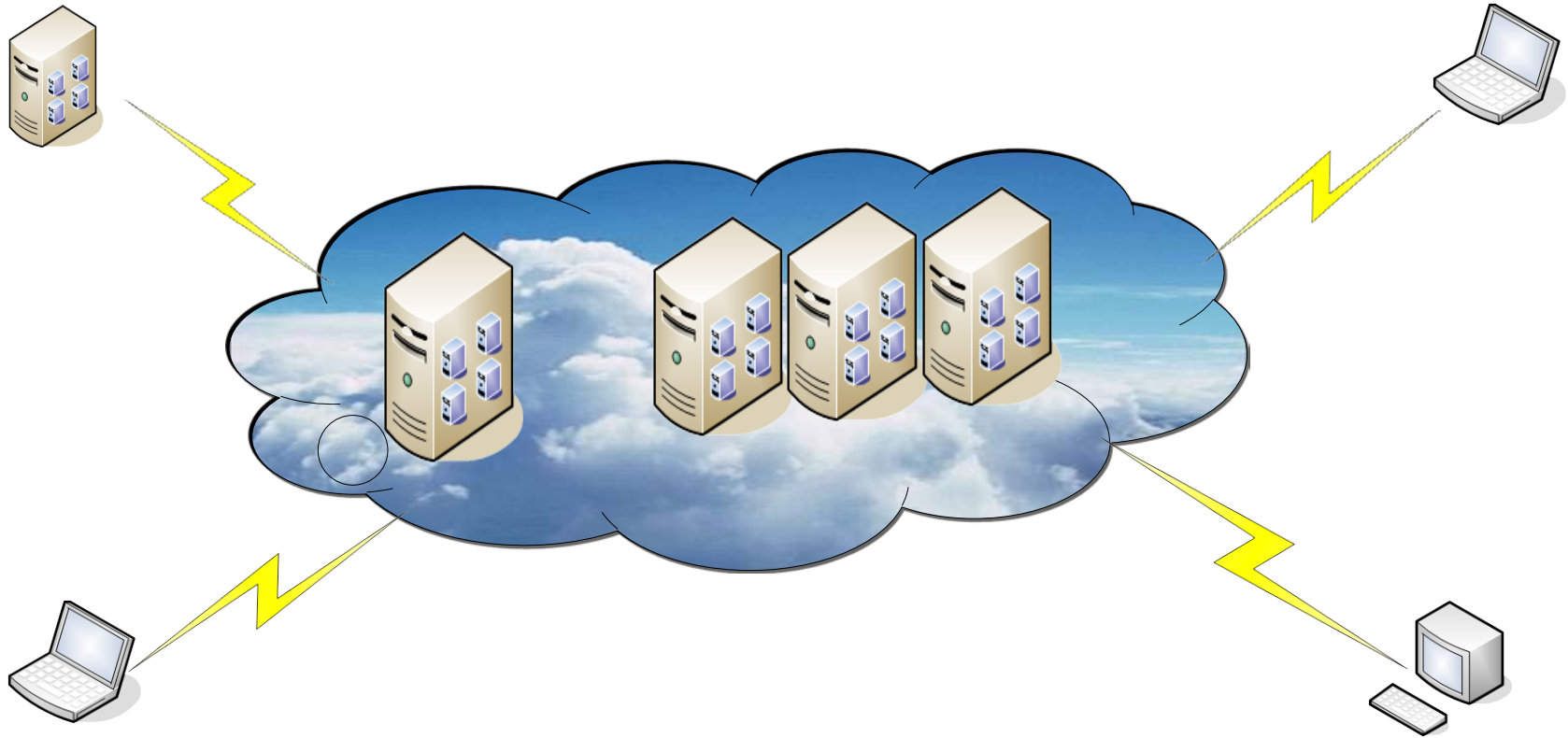
“60% of virtualized servers will be less secure than the physical servers they replace through 2012”

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

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 (Service Oriented Architecture)
- 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

Why Cloud Computing? ...

- Cloud computing could transform the way businesses operate and interact with customers and suppliers.
 - Potential risks have been a major obstacle
 - Use of cloud can reduce risk and be a market differentiator.
- Internal Audit and IT departments that can understand, evaluate, and help to mitigate the risks can help drive the move to the cloud (or slow it down if needed).
- A focus on the following can help reduce the risk of IT projects as use of the cloud will reduce the time and cost (which means less risk):
 - Vendor incentives should be carefully aligned
 - SLAs tightly enforced

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. Salesforce.com, GoogleApps

Platform as a Service
(PaaS)

Application building blocks:
Workflow, Document Management, Data Services, APIs, Fabric, Proprietary Development Languages
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

A thought bubble containing a blue sky with white clouds. The word "Public" is written in the center. There are two small circles on the right side of the bubble.

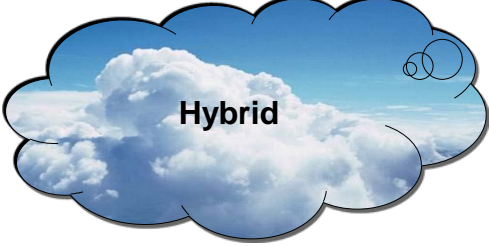
Public

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

A thought bubble containing a blue sky with white clouds. The word "Private" is written in the center. There are two small circles on the left side of the bubble.

Private

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

A thought bubble containing a blue sky with white clouds. The word "Hybrid" is written in the center. There are two small circles on the right side of the bubble.

Hybrid

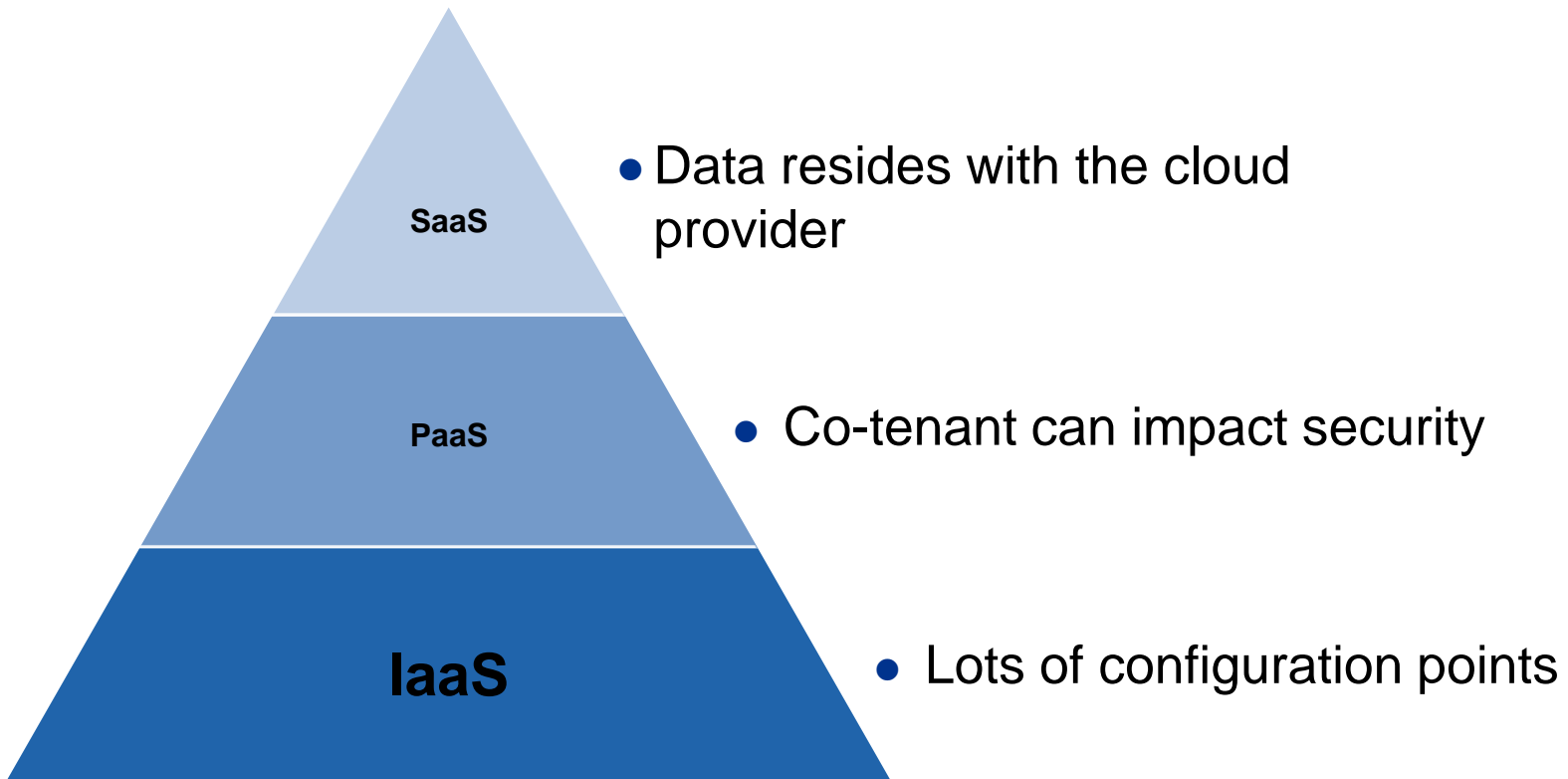
- Bound together that enables data and application portability

A thought bubble containing a blue sky with white clouds. The word "Community" is written in the center. There are two small circles on the left side of the bubble.

Community

- Shared infrastructure for specific community concerns and benefits

Inherent Risks in the Cloud Stack



What do the analysts say?

“Cloud computing combines new technology with unproven vendors and service providers, bringing both business benefits and potential risks. Security, reliability and manageability need to be key elements in the planning and selection processes for cloud services.”

(Gartner – September 2010)

Cloud Computing Challenges

- Loss of physical control
- Security models and standards are still emerging
- Availability concerns
 - Outsourcer ability to react quickly
 - How critical is the application / data that you have on the cloud?
 - Plan for the worst
- Data privacy implications (e.g., data could be in another country)
- Tax implications
- Implications for e-discovery
- ‘Who is responsible for what’ when a security breach happens

Cloud Computing Challenges... (continued)

- Organization's trusted boundaries might be extended
- Isolation/security between virtual machines (competition)
- Customer support practices are evolving
- Guest to host communication happens over the Internet
- Vulnerability of browsers
- Vendor failures notably starts-ups, for e.g., Coghead (9 weeks), MediaMax (script data loss).

Service Outage: Microsoft Online Services (Bus Productivity Online Standard Suite)

The screenshot shows a Microsoft Internet Explorer browser window displaying the Microsoft Online Services Team Blog. The page title is "Microsoft Online Services Team Blog : Response to North America Connectivity Issues". The main content area features a post titled "Response to North America Connectivity Issues" with a 4-star rating. The post text discusses a connectivity issue on January 28, where customers experienced intermittent access to services in the Business Productivity Online Standard Suite. It includes a summary of the issue and a list of actions taken to prevent a recurrence.

Microsoft Online Services TEAM BLOG

HOME EMAIL ABOUT RSS 2.0 ATOM 1.0

Recent Posts

- Webinar: Using the MOSDAL Support Toolkit to diagnose issues with Microsoft Online Services
- Response to North America Connectivity Issues
- What's the Story with SharePoint Online URLs?
- Feature of the Week: Use your Windows Mobile phone with Exchange Online
- Webinar: Using PowerShell with Microsoft Online Services

Tags

Administration Center

Announcements

Blackberry **Business Productivity Online Suite** Buy Services

Deployment Developer Guides

E-mail Entourage Exchange Online

Executive Videos Feature of the

Response to North America Connectivity Issues ★★★★☆

Microsoft Online Services strives to provide exceptional service for all of our customers. On January 28, customers served from a North America data center may have experienced intermittent access to services included in the Business Productivity Online Standard Suite. We apologize for any inconvenience this may have caused you and your employees.

We hold ourselves to the very highest standard. And yesterday, we didn't meet it. The connectivity issue underlined our commitment to service excellence, and all resources were brought to bear to correct and learn from the issue at hand. Within our team, we approach things with a "better every day" attitude; where we will continuously learn and improve to ensure customers can rely on Microsoft now and in the future. This includes customer communication. We are committed to communicating with our customers in an open and honest manner about service issues and the steps we're taking to prevent recurrences. Based on customer feedback, we are actively working to improve our incidence response communications.

In the meantime, this is a summary of yesterday's issue:

- What happened?
 - Monitoring alerted us to a possible issue with networking.
 - Troubleshooting procedures ultimately pointed to a problem with network infrastructure, resulting in intermittent access for customers.
- What actions have been taken to prevent a recurrence?

Service Outages

- Amazon web Services (redundant power system failed)
- Microsoft & Google lost data for 17K and 40K email users respectively
- Virgin Blue Airline (50,000 passengers; availability)
- Workday (15 hours – Payroll / HR) – Customer Service
- Availability expectations & how events are handled

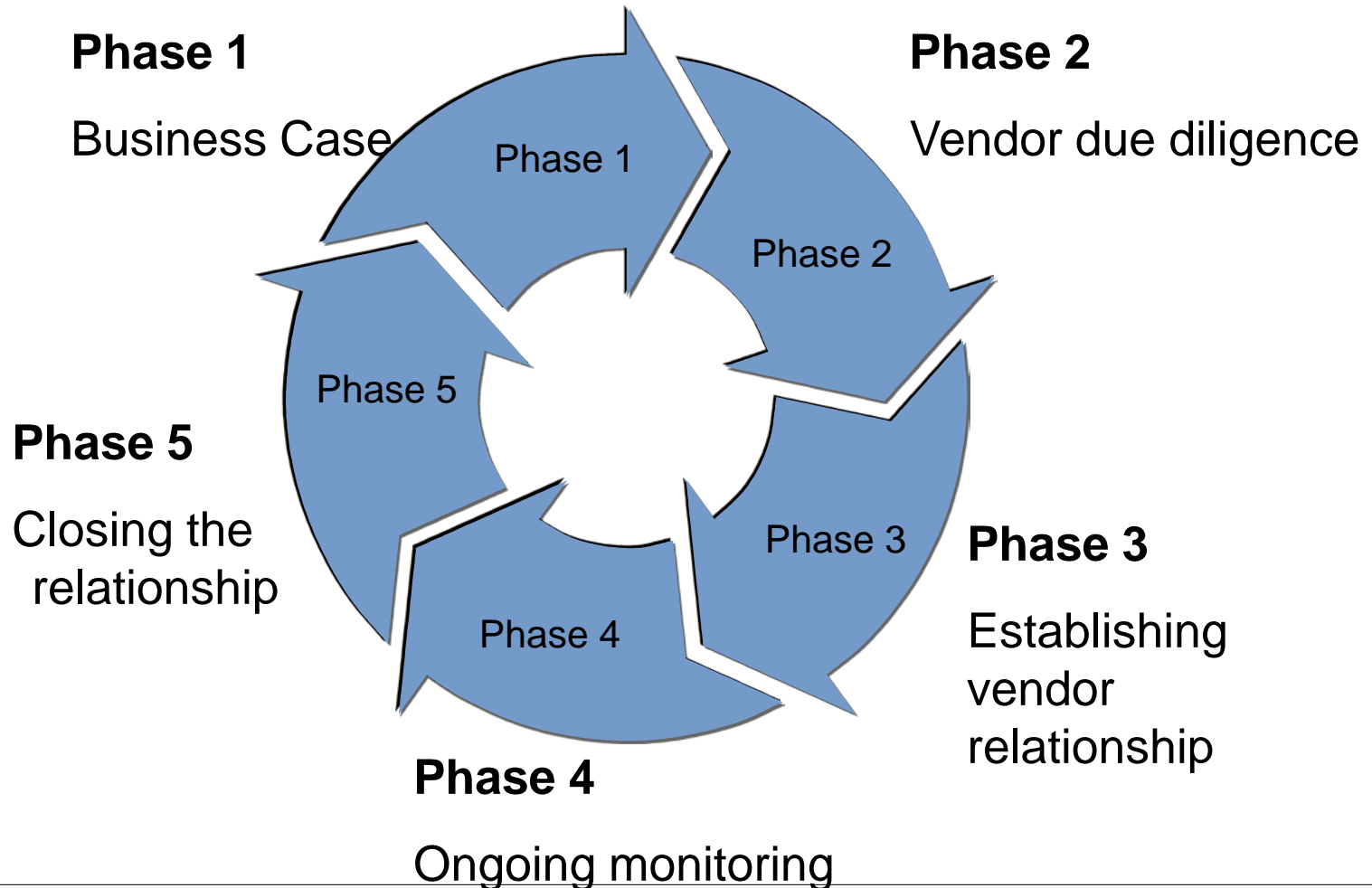
Auditing Cloud Computing Arrangements

How do We Audit the Cloud?

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? If so, what does it cover?

Cloud Outsourcing Lifecycle



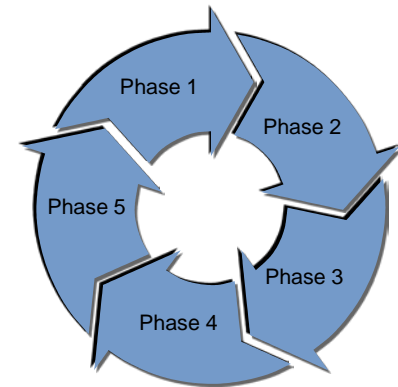
Risk Related Considerations for Each Phase

Phase 1 – Establishing business case

- Is the work core to the organization's business?
- Are there over-riding concerns related to security, privacy, and availability given the nature of the business?

Phase 2 – Vendor due diligence

- Does the technological direction of vendor align with the user organization's direction?
- Is the vendor stable from a finance and operations perspective?



Risk Related Considerations for Each Phase (continued)

Phase 3 – Establishing vendor relationships

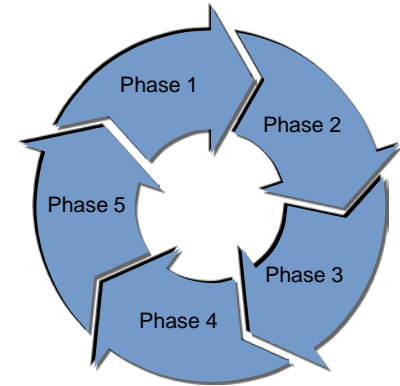
- Are there service-level agreements and escrow?
- Do you know ‘who is responsible for what’?

Phase 4 – Ongoing monitoring

- Does the vendor continue to operate with stability?
- Is there an independent auditor’s report?

Phase 5 – Closing the relationship

- Data transfer and clean up
- Knowledge transfer



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’

**Gartner says SAS 70 is not proof of
security, continuity or privacy compliance”
(July 14, 2010)**

Other approaches

- Other Third party assessments
 - Financial Institution Shared Assessments Program
 - Microsoft Vendor Privacy Assurance Program
 - Payment Card Industry (PCI) Data Security Standards

- Separate reviews conducted by:
 - Internal Audit
 - Vendor management team
 - IT resources

Risk-based Audit Scoping Utilizing RiskIT and COBIT

	COBIT processes and corresponding control objectives that influence all given Risk IT high-level risk scenarios			
	Phases 1, 2	Phases 2, 3	Phase 3	Phases 4, 5
Risk IT Ref # and corresponding High-level Risk Scenarios	Plan and Organize (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)
3. Technology Selection	PO 3.2	AI 1.2		
10. Regulatory compliance				ME 3.1
16. Selection/performance of third-party suppliers	PO 5.5	AI 5.2	DS 2.4	
27. Logical Attacks		AI 2.4	DS 5.10, DS 5.3	
28. Information Media			DS 5.11	
31. Database Integrity			DS 11.6	
32. Logical Trespassing			DS 5.4, DS 5.5	
34. Contract Compliance				ME 3.4

Audit Program : Technology Selection

High-level **Risk** Scenario:
Technology Selection

Relevant COBIT **Control** Objective:
PO 3.2

COBIT Control Objective: Technology Infrastructure Plan – Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources.

Audit Procedure:

- Review the plan to confirm that it includes factors such as consistent integrated technologies, business systems architecture and contingency aspects of infrastructure components, transitional and other costs, complexity, technical risks, future flexibility value, and product/vendor sustainability and directions for acquisition of IT assets.

Finding: User organization has not updated the technology infrastructure plan to reflect the use of an outsourced cloud service provider and its future direction.

Audit Program : Technology Selection (continued)

High-level **Risk** Scenario:
Technology Selection

Relevant COBIT **Control** Objective:
PO 5.5

COBIT Control Objective: Benefit Management – Implement a process to monitor the benefits from providing and maintaining appropriate IT capabilities. IT's contribution to the business, either as a component of IT-enabled investment programs or as part of regular operational support, should be identified and documented in a business case, agreed to, monitored and reported.

Audit Procedure:

- Review the process for developing metrics for measuring benefits (e.g., obtaining guidance from external experts, industry leaders and comparative benchmarking data).
- Inquire whether and confirm that there is a remediation process for identified benefit deviations.

Finding: User organization has not created a formal cost benefit analysis (CBA) or benefit tracking mechanism for utilizing an external Cloud service provider.

Audit Program : Technology Selection (continued)

High-level **Risk** Scenario:
Technology Selection

Relevant COBIT **Control** Objective:
AI 2.4

COBIT Control Objective: Address application security and availability requirements in response to identified risks and in line with the organization's data classification, information architecture, information security architecture and risk tolerance.

Audit Procedure:

- Review application acquisition, implementation and testing plans to confirm that application security and availability within the integrated environment have been addressed.
- Interview business sponsors and review walk-through documentation to assess understanding and adequacy of availability design; inquire whether the design is likely to meet the security and availability requirements.

Findings: Proactive monitoring of the cloud application is not performed. This is particularly relevant for the end-user facing components of the cloud.

Audit Program : Technology Selection (continued)

High-level Risk Scenario: Technology Selection	Relevant COBIT Control Objective: AI 5.2
<p>COBIT Control Objective: Supplier Contract Management – Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organizational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses).</p>	
<p>Audit Procedure:</p> <ul style="list-style-type: none">• Confirm through interviews with key staff members that the policies and standards are in place for establishing contracts with suppliers. Contracts should also include legal, financial, organizational, documentary, performance, security, auditability, intellectual property, responsibility and liability aspects.	
<p>Findings: Cloud provider contract does not include certain critical elements to help protect security and privacy requirements. The contract does not include a non-disclosure agreement, right-to-audit clause, does not address requirements of the state breach notification laws. There is no process for monitoring of potential vendor failure (e.g., Coghead, MediaMax).</p>	

Audit Program : Third-party Performance

High-level **Risk** Scenario:
Third-party Performance

Relevant COBIT **Control** Objective:
DS 2.4

COBIT Control Objective: Supplier Performance Monitoring – Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

Audit Procedure:

- Inspect a sample of supplier service reports to determine if the supplier regularly reports on agreed-upon performance criteria and if performance reporting is objective and measurable and in alignment with defined SLAs and the supplier contract.

Findings: SLAs do not have degree of specificity to allow for effective measurement. Accountability for SLA monitoring has not been established.

Audit Program : Logical Attacks

High-level **Risk** Scenario:
Logical Attacks

Relevant COBIT **Control** Objective:
DS 5.3

COBIT Control Objective: Identity Management – Ensure that all users and their activity on IT systems are uniquely identifiable. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person.

Audit Procedure:

- Determine if access provisioning and authentication control mechanisms are utilized for controlling logical access across all users, system processes and IT resources, for in-house and remotely managed users, processes and systems.

Findings: Generic user ids are used to access the cloud instances. In addition, multi-factor authentication is not utilized for the cloud management console – due to the ease of accessing cloud instances outside the organization’s network multi-factor authentication should be utilized.

Audit Program : Logical Trespassing

High-level **Risk** Scenario:
Logical Trespassing

Relevant COBIT **Control** Objective:
DS 5.4

COBIT Control Objective: User Account Management – Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Perform regular management review of all accounts and related privileges.

Audit Procedure:

- Determine if procedures exist to periodically assess and recertify system and application access and authorities. Determine if access control procedures exist to control and manage system and application rights and privileges according to the organization's security policies and compliance and regulatory requirements.

Findings: Business owner of the cloud has not been defined yet and as a result, the access requests for the cloud instances do not require formal approvals. User organization does not have a process for a periodic independent review of users that have access to the cloud instances. There is no policy/procedure for encryption key management

Audit Program : Logical Trespassing (continued)

High-level **Risk** Scenario:
Logical trespassing

Relevant COBIT **Control** Objective:
DS 5.5

COBIT Control Objective: Security Testing, Surveillance and Monitoring – Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

Audit Procedure:

- Determine if the IT security management function has been integrated within the organization's project management initiatives to ensure that security is considered in development, design and testing requirements, to minimize the risk of new or existing systems introducing security vulnerabilities.

Findings: Network diagrams have not been updated to reflect connectivity with cloud provider. As a result, last network penetration testing did not include this as part of the scope.

Audit Program : Logical Attacks

High-level **Risk** Scenario:
Logical attacks

Relevant COBIT **Control** Objective:
DS 5.10

COBIT Control Objective: Network Security – Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.

Audit Procedure:

- Inquire whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.
- Inquire whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel, and changes to the documentation are tracked in the document history.

Finding: Application teams currently manage the configuration of the cloud firewall instead of relying on the network engineering team.

Audit Program : Information Media

High-level **Risk** Scenario:
Information Media

Relevant COBIT **Control** Objective:
DS 5.11

COBIT Control Objective: Exchange of Sensitive Data – Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

Audit Procedure:

- Inquire whether and confirm that data transmissions outside the organization require encrypted format prior to transmission.
- Inquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.

Findings: Exchange of sensitive data and administration of cloud instances are done via a regular internet connection instead of a secure channel like Secure Socket Layer (SSL) or Secure Shell (SSH).

The organization utilizes an outdated version of Internet Explorer browser software to access and administer the cloud.

Audit Program : Database Integrity

High-level **Risk** Scenario:
Database Integrity

Relevant COBIT **Control** Objective:
DS 11.6

COBIT Control Objective: Security Requirements for Data Management – Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organization's security policy and regulatory requirements.

Audit Procedure:

- Determine whether a policy has been defined and implemented to protect sensitive data and messages from unauthorized access and incorrect transmission and transport, including, but not limited to, encryption, message authentication codes, hash totals, bonded couriers and tamper-resistant packaging for physical transport.

Finding: Personally identifiable information (PII) is stored in clear text at the cloud provider. This is in contravention of HIPAA requirements.

Audit Program : Contract Compliance

High-level Risk Scenario:
Contract Compliance

Relevant COBIT Control Objective:
ME 3.4

COBIT Control Objective: Positive Assurance of Compliance – Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.

Audit Procedure:

- Inquire whether procedures are in place to regularly assess levels of compliance with legal and regulatory requirements by independent parties.
- Review policies and procedures to ensure that contracts with third-party service providers require regular confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.

Finding: Cloud computing vendor does not have an independent auditor's report, for e.g., a SAS70 report, a WebTrust report, or a SysTrust report.

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
- Cloud can reduce risk and transform the way your business operates
- It can be a strategic differentiator

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
http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf
- 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
- InformationWeek http://www.informationweek.com/cloud-computing/blog/archives/2009/02/lessons_from_th.html?catid=cloud-computing
- Outsourced IT Environments – Audit/Assurance Program (ISACA)
- Cloud Computing Paradigm Change - <http://www.kpmg.com/CH/en/Library/KPMG-in-the-Media/Pages/Cloud-Computing-offers-paradigm-change.aspx>

References (continued)

Questions?

Presenter's Contact Details

Heather Paquette

KPMG LLP

+1 (312) 665 8943

hcpaquette@kpmg.com

www.kpmg.com

Tom Humbert

KPMG LLP

+1 (312) 665 1593

thumbert@kpmg.com

www.kpmg.com

Thank You



cutting through complexity™

© 2010 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. 43713CHI

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International Cooperative (“KPMG International”).