Cloud Computing:

Background, Risks and Audit Recommendations

October 30, 2014
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Computing: Overview</td>
<td>3</td>
</tr>
<tr>
<td>Multiple Models of Cloud Computing</td>
<td>11</td>
</tr>
<tr>
<td>Deployment Models</td>
<td>16</td>
</tr>
<tr>
<td>Considerations For Moving To The Cloud</td>
<td>21</td>
</tr>
<tr>
<td>Risks</td>
<td>32</td>
</tr>
<tr>
<td>Cloud Computing Audit Approach</td>
<td>49</td>
</tr>
<tr>
<td>Appendix</td>
<td>69</td>
</tr>
</tbody>
</table>
Cloud Computing: Overview
Cloud Computing - Definition

Cloud Computing describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources.

These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption.

Key Features

- On demand self service
- Standardized IT based capability
- Rapid Elasticity
- Web based accessibility & flexibility
- Location independent resource pooling
- Scalability & resilience as key design components
- Prices on a consumption based model
- Ubiquitous network access
# Essential Characteristics Of Cloud Computing

According to National Institute of Standards and Technology (NIST), the five essential characteristics of cloud computing are:

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-Demand Self Service</strong></td>
<td>Authorized agencies must be able to provide and release capabilities, as needed, automatically, without requiring human interaction with each services provider.</td>
</tr>
</tbody>
</table>
The Latest Evolution Of Hosting

Cloud Computing Drivers and Inhibitors

**Pay-as-you-go**

- Immediately scalable

**Drivers**

- Increased ROI
- Quicker payback
- Lower upfront investment
- Accelerated deployment
- Greater flexibility and scalability
- Focus on core competencies

**Cloud characteristics**

**Multi-tenant**

- Highly abstracted

**Inhibitors**

- Security, control and compliance concerns
- Resistance to IT change
- One size fits all approach
Top 5 Reasons For Moving To The Cloud

- Get Access to the newest functionality faster: 41.3%
- Increase revenue by enabling us to build new revenue generating products and services faster: 40.5%
- Improve Resource Utilization: 40.4%
- Reduce The total size of IT Budget: 40.3%
- Give Business units more direct control over sourcing their own IT Solutions: 39%

*Percentage Respondents
*n = 1,109
*Source: IDC's CloudTrack Survey, October 2013
Moving to cloud-based systems not only has many benefits but also is accompanied by some challenges that need to be addressed.

- **Security Concerns**: 49%
- **Regulatory or Compliance Issues**: 35.3%
- **Reliability concerns in terms of service availability**: 32.9%
- **Concerns cloud cannot support the operational Requirements**: 32.3%
- **IT Governance issues including challenges related to defining standard services**: 31%
- **Immaturity of cloud**: 30.7%

*Percentage Respondents

- n = 1,109
- Source: IDC’s CloudTrack Survey, October 2013*
Multiple Models of Cloud Computing
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 more simply, “IT runs over the Internet instead of installing hardware and software yourself.”

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

Service Models
- **Business Process as a Service** (emerging)
  - Entire business process as a service in the cloud
- **Software as a Service**
  - Finished applications that you rent and customize
- **Platform as a Service**
  - Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity
- **Infrastructure as a Service**
  - Deployment platform that abstracts the infrastructure

Deployment Models
- Public Cloud
- Community Cloud
- Hybrid Cloud
- Private Cloud
Cloud Computing Offerings

* A sample list only. There are many more players.
Public Cloud – Buyer Preference by Providers

- AWS
  - Already Using: 27%
  - Aware of and likely to consider: 19%
  - Aware of and not considering: 27%
  - Not aware: 27%

- Google
  - Already Using: 19%
  - Aware of and likely to consider: 37%
  - Aware of and not considering: 35%
  - Not aware: 9%

- Microsoft
  - Already Using: 17%
  - Aware of and likely to consider: 38%
  - Aware of and not considering: 37%
  - Not aware: 8%

- AT&T
  - Already Using: 7%
  - Aware of and likely to consider: 27%
  - Aware of and not considering: 34%
  - Not aware: 32%

- Rackspace
  - Already Using: 7%
  - Aware of and likely to consider: 36%
  - Aware of and not considering: 35
  - Not aware: 22

- Verizon-Terremark
  - Already Using: 5%
  - Aware of and likely to consider: 20%
  - Aware of and not considering: 34
  - Not aware: 41

- IBM
  - Already Using: 5%
  - Aware of and likely to consider: 35
  - Aware of and not considering: 46
  - Not aware: 14

- CenturyLink-Savvis
  - Already Using: 4%
  - Aware of and likely to consider: 12
  - Aware of and not considering: 32
  - Not aware: 52

- HP
  - Already Using: 4%
  - Aware of and likely to consider: 33
  - Aware of and not considering: 45
  - Not aware: 18

- CSC
  - Already Using: 2%
  - Aware of and likely to consider: 9
  - Aware of and not considering: 31
  - Not aware: 58

- Joyent
  - Already Using: 2%
  - Aware of and likely to consider: 11
  - Aware of and not considering: 44
  - Not aware: 43

- GoGrid
  - Already Using: 1%
  - Aware of and likely to consider: 13
  - Aware of and not considering: 32
  - Not aware: 54

- Percentage Respondents
- n = 101

Source: Everest Group, Enterprise Cloud Adoption Survey 2013
Cloud Usage – How Can It Help Businesses Operationally?

- Allowing High Variable Demand - Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis
- Reaching Geographically Dispersed Users
- Consolidating Company IT
- Planning for Disaster Recovery
- Decoupling and separation of the business service from the infrastructure needed to run it (virtualization)
- Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts
- Cost allocation flexibility for customers wanting to move CapEx into OpEx
- Reduced costs due to operational efficiencies, and more rapid deployment of new business services
- Operational Expertise – Patch Management, Version Updates, Data Security Management
Cloud Usage – How The Cloud Is Being Utilized?

Source: Skyhigh Cloud Adoption Risk Report Q1 2014
A Shift Toward Decentralized, Vertical, Subscription-Based Buying

The broader software implementation trends illustrate how enterprises are already changing their approach to purchasing applications and IT.

<table>
<thead>
<tr>
<th>Approach to Software Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vertical Specific software n=532</strong></td>
</tr>
<tr>
<td>SaaS: 16</td>
</tr>
<tr>
<td><strong>Web Conferencing, Collaboration/Social Software Suites n=582</strong></td>
</tr>
<tr>
<td>SaaS: 17</td>
</tr>
<tr>
<td><strong>Enterprise Control Management n=473</strong></td>
</tr>
<tr>
<td>SaaS: 17</td>
</tr>
<tr>
<td><strong>Digital Content Creation n=442</strong></td>
</tr>
<tr>
<td>SaaS: 15</td>
</tr>
<tr>
<td><strong>Office suites n=688</strong></td>
</tr>
<tr>
<td>SaaS: 19</td>
</tr>
<tr>
<td><strong>Project and Portfolio Management n=541</strong></td>
</tr>
<tr>
<td>SaaS: 18</td>
</tr>
<tr>
<td><strong>Customer relationship management n=596</strong></td>
</tr>
<tr>
<td>SaaS: 20</td>
</tr>
<tr>
<td><strong>Supply chain management n=481</strong></td>
</tr>
<tr>
<td>SaaS: 18</td>
</tr>
<tr>
<td><strong>Enterprise resource planning n=529</strong></td>
</tr>
<tr>
<td>SaaS: 17</td>
</tr>
<tr>
<td><strong>Business Intelligence n=517</strong></td>
</tr>
<tr>
<td>SaaS: 15</td>
</tr>
</tbody>
</table>

**Question Asked:** What was the chosen approach for the implementation of those software applications?

**Base:** Respondents are piloting or have deployed the software application enterprise wide and/or in some business units. Percentages may not add up to 100% because of rounding.

**Source:** Market Trends Application
Most Used Applications In The Public Cloud

SaaS is a turnkey service, with application, presentation, and data tiers and all associated services in a single service that can be accessed and provisioned over the Internet.

- **CRM Applications (Marketing/sales)**: 21.2%
- **CRM Applications (Call Centers/Contact Centers)**: 20.9%
- **Supply Chain & Logistics**: 19.6%
- **Human Resource Application**: 19.3%
- **Financial/Accounting Applications**: 18.9%

*Percentage Respondents*

- $n = 1,109$

*Source: IDC's CloudTrack Survey, October 2013*
Cloud Adoption by Company Size

- **< 20 Employees**
  - Cloud Adoption: 68%
  - Non-Cloud Adoption: 6%

- **20-99 Employees**
  - Cloud Adoption: 61%
  - Non-Cloud Adoption: 7%

- **100-249 Employees**
  - Cloud Adoption: 66%
  - Non-Cloud Adoption: 9%

- **250-499 Employees**
  - Cloud Adoption: 50%
  - Non-Cloud Adoption: 11%

- **500+ Employees**
  - Cloud Adoption: 53%
  - Non-Cloud Adoption: 9%

Source: Infographic: SMB Cloud Adoption Trends in 2014
Cloud Maturity SMB vs Enterprise

**SMB**
- Developing a cloud strategy: 20%
- Working on first cloud project: 29%
- Multiple projects & developing apps in the cloud: 25%
- Heavily using cloud infrastructure: 26%

**Enterprise**
- Developing a cloud strategy: 16%
- Working on first cloud project: 35%
- Multiple projects & developing apps in the cloud: 31%
- Heavily using cloud infrastructure: 18%

*Source: Infographic: SMB Cloud Adoption Trends in 2014*
Market Forecast
Cloud Services Market Outlook

**Cloud IT Spending Soars**

Global spending forecast by enterprises on cloud architecture

<table>
<thead>
<tr>
<th>$:\text{in billions}$</th>
<th>'11</th>
<th>'12</th>
<th>'13</th>
<th>'14e</th>
<th>'15e</th>
<th>'16e</th>
<th>'17e</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{200}$</td>
<td>50</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>250</td>
<td>300</td>
<td>350</td>
</tr>
</tbody>
</table>

Source: IHS

**Cloud Applications Will Account for 90 Percent of Mobile Data Traffic by 2018**

<table>
<thead>
<tr>
<th>Year</th>
<th>Mobile Non-Cloud Traffic</th>
<th>Mobile Cloud Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>82%</td>
<td>18%</td>
</tr>
<tr>
<td>2014</td>
<td>83%</td>
<td>17%</td>
</tr>
<tr>
<td>2015</td>
<td>85%</td>
<td>15%</td>
</tr>
<tr>
<td>2016</td>
<td>86%</td>
<td>14%</td>
</tr>
<tr>
<td>2017</td>
<td>88%</td>
<td>12%</td>
</tr>
<tr>
<td>2018</td>
<td>90%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Cisco VNI Mobile, 2014

*Source: Investors’ Business Daily*
Cloud Services Market Outlook

Cloud service revenue is expected to be USD 220bn by 2015, and USD 480bn by 2019

Business processes (cloud-based advertising, e-commerce, human resources, payment processing and other business processes) cloud services market is expected to be USD 370bn by 2019

Data from Intuit and Emergent Research reveals that by 2020, 78 percent of small businesses will be “fully adapted” to cloud computing. That’s more than double the current 37 percent adoption rate as of 2014.

Source: Research Pedia; Small Business Trends
Cloud Services Market Outlook

Cisco predicts Cloud Data Center traffic to grow at 35% CAGR. By 2017, over two-thirds of all data center traffic is expected to be based in the cloud.

Risks
Clouds Are Cloudy

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?
- Does backup happen? How? Where?

... security, compliance, and value are lost as well.
Top Risks

- Loss of Governance
- Lock-In
- Management Interface Compromise
- Incomplete or Insecure Data Deletion
- Data Protection
- Malicious Insider / Investigative Support
- Isolation Failure
- Compliance Risks
Categories of Control Objectives

- Compliance
- Data Governance
- Facility Security
- Human Resources
- Information Security
- Legal
- Operations Management
- Risk Management
- Release Management
- Resiliency
## Control Objectives

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Independent Regulatory Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Vendor Management</td>
</tr>
<tr>
<td></td>
<td>Information System Regulatory Mapping</td>
</tr>
<tr>
<td></td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>Data Governance</td>
<td>Classification</td>
</tr>
<tr>
<td></td>
<td>Handling / Labeling / Security Policy</td>
</tr>
<tr>
<td></td>
<td>Retention Policy</td>
</tr>
<tr>
<td></td>
<td>Risk Assessments</td>
</tr>
<tr>
<td>Facility</td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>User Access</td>
</tr>
<tr>
<td></td>
<td>Asset Management</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Background Screening</td>
</tr>
<tr>
<td></td>
<td>Employment Agreements</td>
</tr>
<tr>
<td></td>
<td>Employment Termination</td>
</tr>
</tbody>
</table>
## Control Objectives

<table>
<thead>
<tr>
<th>Information Security</th>
<th>Management Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Policy, Reviews, Enforcement</td>
</tr>
<tr>
<td></td>
<td>User Access Restriction / Authorization / Reviews</td>
</tr>
<tr>
<td></td>
<td>Awareness Training</td>
</tr>
<tr>
<td></td>
<td>Roles / Responsibilities</td>
</tr>
<tr>
<td></td>
<td>Management Oversight</td>
</tr>
<tr>
<td></td>
<td>User Access Policy</td>
</tr>
<tr>
<td></td>
<td>Workspace Cleanliness</td>
</tr>
<tr>
<td></td>
<td>Anti-Virus / Malicious Software</td>
</tr>
<tr>
<td></td>
<td>Incident Management – Identification, Reporting and Monitoring</td>
</tr>
<tr>
<td></td>
<td>Incident Response Legal Preparation</td>
</tr>
</tbody>
</table>
### Control Objectives

<table>
<thead>
<tr>
<th>Category</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal</strong></td>
<td>Non-Disclosure Agreements</td>
</tr>
<tr>
<td></td>
<td>Third Party Agreements</td>
</tr>
<tr>
<td></td>
<td>Service Level Agreements</td>
</tr>
<tr>
<td><strong>Operations Management</strong></td>
<td>Capacity / Resource Planning</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>Program</td>
</tr>
<tr>
<td></td>
<td>Assessments</td>
</tr>
<tr>
<td></td>
<td>Mitigation / Acceptance</td>
</tr>
<tr>
<td></td>
<td>Business / Policy Change Impacts</td>
</tr>
<tr>
<td></td>
<td>Third Party Access</td>
</tr>
<tr>
<td><strong>Release Management</strong></td>
<td>Production Changes</td>
</tr>
<tr>
<td></td>
<td>Outsourced Development</td>
</tr>
<tr>
<td><strong>Resiliency</strong></td>
<td>Management Program</td>
</tr>
<tr>
<td></td>
<td>Impact Analysis</td>
</tr>
<tr>
<td></td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td></td>
<td>Business Continuity Testing</td>
</tr>
</tbody>
</table>
Cloud Computing Audit Approach
Involvement of Internal Audit in Cloud Computing

<table>
<thead>
<tr>
<th>Vendor Selection &amp; Contract Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Validation of business case</td>
</tr>
<tr>
<td>• Right to Audit Clause and/or SSAE16</td>
</tr>
<tr>
<td>• Compliance Scope</td>
</tr>
<tr>
<td>• Impact of Regulations on Data Security</td>
</tr>
<tr>
<td>• Stability of Partners and Services Providers</td>
</tr>
<tr>
<td>• Contractual Data Protection Responsibilities and Related Clauses</td>
</tr>
<tr>
<td>• Impact of Regulations on Provider Infrastructure</td>
</tr>
<tr>
<td>• Prepare Evidence of How Each Requirement Is Being Met</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pre-Implementation Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Project management - roles and responsibilities</td>
</tr>
<tr>
<td>• Data migration strategy</td>
</tr>
<tr>
<td>• Inherent and residual risk assessment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Post-Implementation Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Accuracy of data</td>
</tr>
<tr>
<td>• Policies and procedures pertaining to data security, privacy of data</td>
</tr>
<tr>
<td>• Regulatory changes - HIPAA, PCI, etc.</td>
</tr>
</tbody>
</table>
Audit/Projects Around Cloud Computing

- Cloud computing platform evaluation / due diligence
- Data migration review to the new platform
- Management of the cloud computing function
- Security reviews
  - Security of data
  - Network accessibility
  - User administration
- Regular review of SOC Type 1/provider sponsored audit reports
- Cost/Savings impact
- Realignment of controls for regulatory reporting
- SLA/KPI review to ensure the provider is living up to their end of the bargain
- Impacts to Disaster Recovery/Business Continuity
Scoping

**Define the audit objectives and scope. Understand the core business process and its alignment with IT, in its non-cloud form and current or future cloud implementation.**

- Obtain a description of all cloud computing environments in use and under consideration.
- Obtain a description of all cloud computing applications in use and under consideration.
- Identify the types of cloud services (IaaS, PaaS, SaaS) in use and under consideration, and determine the services and business solutions to be included in the review.
- Obtain and review any previous audit reports with remediation plans. Identify open issues, and assess updates to the documents with respect to these issues.

**Since the areas under review rely heavily on the effectiveness of core IT general controls, it is recommended that audit/assurance reviews of the following areas be performed prior to the execution of the cloud computing review, so that appropriate reliance can be placed on these assessments:**

- Identity management (if the organization’s identity management system is integrated with the cloud computing system)
- Security incident management (to interface with and manage cloud computing incidents)
- Network perimeter security (as an access point to the Internet)
- Systems development (in which the cloud is part of the application infrastructure)
- Project management
- IT risk management
- Data management (for data transmitted and stored on cloud systems)
- Vulnerability management
Audit Approach

The ISACA approach breaks down an audit into two categories

- Governing the Cloud
- Operating in the Cloud

Each area has Control Objectives that are subsequently reviewed.
Audit Approach

Governing the Cloud includes the following processes. The controls associated with these processes are then evaluated.

**Governance**

- Audit/Assurance Objective: Governance functions are established to ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability.

**Enterprise Risk Management**

- Audit/Assurance Objective: Risk management practices are implemented to evaluate inherent risks within the cloud computing model, identify appropriate control mechanisms, and ensure that residual risk is within acceptable levels.

**Information Risk Management**

- Audit/Assurance Objective: A process to manage information risk exists and is integrated into the organization’s overall ERM framework. Information risk management information and metrics are available for the information security function to manage risks within the risk tolerance of the data owner.
## Audit Approach

*Governing the Cloud includes the following processes.*

### Third-party Management

- **Audit/Assurance Objective:** The customer recognizes the outsourced relationship with the service provider. The customer understands its responsibilities for controls, and the service provider has provided assurances of sustainability of those controls.

### Contractual Obligations

- **Audit/Assurance Objective:** The service provider and customer establish bilateral agreements and procedures to ensure contractual obligations are satisfied, and these obligations address the compliance requirements of both the customer and service provider.

### Legal Compliance

- **Audit/Assurance Objective:** Legal issues relating to functional, jurisdictional and contractual requirements are addressed to protect both parties, and these issues are documented, approved and monitored.

### Right to Audit

- **Audit/Assurance Objective:** The right to audit is clearly defined and satisfies the assurance requirements of the customer’s board of directors, audit charter, external auditors and any regulators having jurisdiction over the customer.
Audit Approach

*Governing the Cloud includes the following processes.*

<table>
<thead>
<tr>
<th>Auditability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Audit/Assurance Objective: The service provider’s operating environment should be subject to audit to satisfy the customer’s audit charter, compliance requirements and good practice controls without restriction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Audit/Assurance Objective: The use of cloud computing does not invalidate or violate any customer compliance agreement.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO 27001 Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Audit/Assurance Objective: Service provider security assurance is provided through ISO27001 Certification.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Transition Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Audit/Assurance Objective: Planning for the migration of data, such as formats and access, is essential to reducing operational and financial risks at the end of the contract. The transition of services should be considered at the beginning of contract negotiations.</td>
</tr>
</tbody>
</table>
Audit Approach

*Operating in the Cloud includes the following processes. The controls associated with these processes are then evaluated.*

**Incident Response, Notification and Remediation**
- Audit/Assurance Objective: Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.

**Application Security Architecture**
- Audit/Assurance Objective: Applications are developed with an understanding of the interdependencies inherent in cloud applications, requiring a risk analysis and design of configuration management and provisioning process that will withstand changing application architectures.

**Compliance**
- Audit/Assurance Objective: Compliance requirements are an integral component of the design and implementation of the application security architecture.
Audit Approach

Operating in the Cloud includes the following processes.

**Tools and Services**
- Audit/Assurance Objective: Use of development tools, application management libraries and other software are evaluated to ensure their use will not negatively impact the security of applications.

**Application Functionality**
- Audit/Assurance Objective: For SaaS implementations, the application outsourced to the cloud contains the appropriate functionality and processing controls required by the customer’s control policies within the processing scope (financial, operational, etc.).

**Encryption**
- Audit/Assurance Objective: Data are securely transmitted and maintained to prevent unauthorized access and modification.
Audit Approach

Operating in the Cloud includes the following processes.

Key Management

- Audit/Assurance Objective: Encryption keys are securely protected against unauthorized access, separation of duties exists between the key managers and the hosting organization, and the keys are recoverable.

Identity and Access Management

- Audit/Assurance Objective: Identity processes assure only authorized users have access to the data and resources, user activities can be audited and analyzed, and the customer has control over access management.

Virtualization

- Audit/Assurance Objective: Virtualization operating systems are hardened to prevent cross-contamination with other customer environments.
At A Minimum: Execute A Cloud Service Provider Questionnaire

• **Ask the basic questions…**
  – Where do you store our data?
  – Who can access and retrieve the data?
  – Do you have auditing enabled? Is it available to us?
  – How do you determine if our data has been tampered with?
  – What are your configuration standards?
  – Does backup happen? How? Where?
  – Have you attained any external/independent security certifications?

• **Follow-up with a detailed information security questionnaire**
Ensure Basic Mitigation Techniques Are In Place

**Intellectual Property Loss**

- Monitoring controls
- Encryption design and requirements
- Data backup management

**Compliance Reporting**

- Specify a breach notification process
- Ask for independent reviews and certifications
- Use your own “Golden Rule” – Treat my data like I treat my own

**Security Administration**

- Analyze the cloud service provider (CSP) security model
- Ensure strong authentication and access controls
- Require the CSP to be completely transparent
Q & A
Thank You

Cal Slemp
Managing Director
New York, NY
+1.203.905.2926
cal.slemp@protiviti.com
Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.