Cloud Computing

Key Risks and Management’s Role
## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Context Setting: Cloud &amp; The Growing Business/IT Gap</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Common Cloud Risks</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>Cloud Governance and the Role of Management</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>Conclusions and Q&amp;A</td>
<td>54</td>
</tr>
</tbody>
</table>
What is Cloud Computing
What is Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.
What is Cloud Computing?

Cloud computing is a general term for anything that involves delivering hosted services over the Internet.
What is Cloud Computing
What is Cloud Computing

Types of Cloud Computing

- Public Cloud
  - Don’t own the assets (Amazon, Google, etc.)
- Private Cloud
  - More costs, more controls
  - Host in own data centre or third party
- Hybrid Cloud
  - Blend between Public and Private Cloud
What is Cloud Computing

Models of Cloud Computing services

• Infrastructure as a service (IAAS)
• Platform as a service (PAAS)
• Software as a service (SAAS)
What is Cloud Computing

“PaaS”

**Cloud Enablers**

- Mgmt. and Security

**V-Cloud**

**SaaS**

- "PaaS"

**IaaS**

- System Infrastructure Services
- App. Infrastructure Services
- Application Services
- Information Services
- Business Services

**Small**

- Google
- salesforce.com
- Microsoft Dynamics
- Oracle
- LotusLive
- Workday
- NetSuite

**Large**

- force.com
- Appian
- Appian
- Rollbase
- BungeeConnect
- LongJump
- VMware
- Amazon Web Services
- V-Cloud
- IBM
- RSA
- RSA
- CA
- Oracle

**Application Services**

- force.com
- Appian
- Rollbase
- BungeeConnect
- Google
- Microsoft Dynamics
- Oracle
- LotusLive
- Workday
- NetSuite

**Information Services**

- force.com
- Appian
- Rollbase
- BungeeConnect
- Google
- Microsoft Dynamics
- Oracle
- LotusLive
- Workday
- NetSuite

**Business Services**

- force.com
- Appian
- Rollbase
- BungeeConnect
- Google
- Microsoft Dynamics
- Oracle
- LotusLive
- Workday
- NetSuite

**System Infrastructure Services**

- force.com
- Appian
- Rollbase
- BungeeConnect
- Google
- Microsoft Dynamics
- Oracle
- LotusLive
- Workday
- NetSuite
What is cloud computing?

- A game-changing technology model and paradigm
- Ubiquitous, convenient, on-demand, pay-as-you-go network access to a shared pool of configurable computing resources
- Major technology and business disrupter (cost reduction and innovation)
- **Security impact:** Driving new risks and security concerns that impacts all elements of the business ecosystem

### Essential Characteristics

<table>
<thead>
<tr>
<th>On-Demand Service</th>
<th>Broad Network Access</th>
<th>Resource Pooling</th>
<th>Rapid Elasticity</th>
<th>Measured Service</th>
</tr>
</thead>
</table>

### Service Models

<table>
<thead>
<tr>
<th>Infrastructure as a Service (IaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Software as a Service (SaaS)</th>
<th>Business Process as a Service (BPaaS)</th>
</tr>
</thead>
</table>

### Deployment Models

<table>
<thead>
<tr>
<th>PUBLIC</th>
<th>PRIVATE</th>
<th>HYBRID</th>
<th>COMMUNITY</th>
</tr>
</thead>
</table>
**Platform Overview**

**Benefits**
- Innovate with Agile Solutions
  - Flexible IT Infrastructure
  - Alignment with Business Demands
- Lower Capital Costs
  - Shared Resources
  - Pay-per-use
- Faster time to Market
  - Self Service
  - Faster Provisioning of services
  - Scale up or down services

**Service Platforms**
- **Infrastructure as a Service (IaaS)**
  - Manage Compliance with Laws and Regulations
  - Manage Data Security
  - Manage Access to Applications/Data
  - Manage Application Services
  - Manage System Infrastructure Services
  - Manage Security Processes
- **Platform as a Service (PaaS)**
  - Manage Compliance with Laws and Regulations
  - Manage Data Security Requirements
  - Manage Application Services
  - Manage Access to Applications
- **Software as a Service (SaaS)**
  - Manage Compliance with Laws and Regulations
  - Manage Access and Changes to Applications/Data

**Responsibilities**
- Manage Compliance with Laws and Regulations
- Manage Data Security
- Manage Access and Changes to Applications/Data
Knowledge Check

• True or False

Software as a Service is an offering which provides elastic on-demand computing infrastructure to customers.
**Sanity Check**

**Panel 1:**
I need you to explain the concept of the hybrid cloud in simple terms.

**Panel 2:**
A hybrid cloud is a technology you don't understand combined with another one.
COMMON CLOUD RISKS
High-Level Cloud Risks:

- **Business case** - The benefits and cost savings may be overstated and does not consider ongoing risks and operating costs.

- **Data ownership** - Ambiguity about who owns the data (e.g. trade secrets, intellectual property, customer records) in the cloud.

- **Data security** - Inability to enforce enterprise security policies in the cloud provider’s environment and trust the security measures within the cloud.

- **Sovereignty** - Lack of clarity around which country and legal jurisdiction has rights over the data in the cloud.

- **Assurance** - Inability to obtain sufficient assurance on controls within the cloud provider’s environment.
Cloud Risk Framework – Detailed View

1. Strategy & business case
   - Strategic oversight of IT enablement & support
   - Business value focused
   - Risk aware & balanced business cases

2. Business requirements
   - Business stakeholder driven & acceptance model
   - Cross functional engagement & alignment

3. Compliance
   - Agile, adaptive, & holistic, compliance management
   - Business stakeholder accountability
   - Improved continuous compliance readiness

4. Legal contract terms & SLAs
   - Reduced legal risk
   - Terms & conditions completeness & verifiability
   - Continuous vendor risk & compliance alignment

5. Asset & data governance
   - Data classification driven
   - Baseline security
   - Data lifecycle management
   - Improved policy efficacy

6. Information & data management
   - Embedded security for architecture & operations
   - Cloud services lifecycle risk management

7. Continuity & resiliency
   - Enhanced confidence in cloud provider reliability
   - External business dependency clarity

8. Technology & service provider governance
   - Vendor risk due diligence automation & scalability
   - “Shadow IT” revelations
   - Improved understanding of actual business user needs

9. Service orchestration & interoperability
   - Enterprise architecture collaboration for platform enablement & compatibility
   - Non-proprietary & innovation transformation enablement

10. IT operations management
    - IT service management control & automation
    - Operational excellence in cloud service monitoring & support
Lack of strategic direction and supporting business cases to balance the value proposition of the cloud services delivery model, and related subscription cost model, against the potential for introducing unacceptable business risks or violating corporate policies critical to sustaining the organization.
Domain 2. Business Requirements

Business decisions to adopt cloud services are formed by incomplete business requirements resulting in cloud service subscription cost commitments that do not satisfy the business need or cause a violation of corporate policy, posing an unacceptable business risk to the organization.
Compliance and audit programs are not scalable or holistically managed to satisfy the overlapping, evolving and complex landscape of requirements sourced from legal, regulatory, and other external obligations or internal corporate policies resulting in penalties, loss of trust, or inability to meet business requirements due to the adoption of cloud services.
Domain 4. Legal Contract Terms & SLAs

Service level agreements (SLAs) or other contractual commitments are agreed to that conflict with or exclude pre-existing essential business requirements or result in non-adherence to internal corporate policies, industry acceptable standards, legal, regulatory or other external obligations.
Permissible or restrictive usage and treatment of business critical assets and the lifecycle and protection of corporate or third party entrusted data is not defined to derive information security baseline requirements for authorizing the adoption of cloud services.
Corporate policy and risk management measures do not account for or address adverse information security or data breach events caused by inappropriate access to, use and treatment of business critical assets and corporate or third party entrusted data impacted by cloud services.
Reliability needs, performance thresholds and contingency considerations for business critical dependencies on cloud services are not defined to establish business requirements for preparing for or adequately responding to potential business disruptions or loss of service.
Lack of visibility into periodic or real-time monitoring of enterprise-wide cloud service thresholds, service level adherence, and risk and compliance impacts (e.g., emerging information security threat vectors) results in the following:

- unknown business risks;
- non-adherence to contract terms and service level commitments;
- internal policy and regulatory compliance violations; or
- unintended expansion of unauthorized cloud services.
Opportunities for business value enhancements are constrained by legacy, proprietary or incompatible technologies that do not accommodate the ability to integrate a broad portfolio of cloud services.
Opportunities for enhanced business capability and agility are constrained by unsatisfactory management of integrated cloud services platform by cloud services operations function.
Knowledge Check

• True or False

Lack of clarity around which country and legal jurisdiction has rights over the data in the cloud is a risk associated with cloud computing?
Sanity Check

I migrated our northern data center to the cloud.

But the cloud stopped working and I can’t find the phone number for our cloud guy.

So… whatever.

You lost our data center?

That’s one way to look at it.
CLOUD GOVERNANCE
An appropriate Cloud governance structure is essential to move organizations toward greater cloud service awareness and a trusted, organized, and predictable approach to cloud use.
Cloud Governance

Business use of cloud services continues to increase, yet many businesses have no idea how many and which cloud services—authorized or not—are actually in use across their enterprises.
This lack of knowledge challenges organizations’ ability to adequately address the risks associated with cloud services, including data security, customer privacy, reliability of critical business processes, and compliance risks.
Cloud Governance

As cloud adoption continues growing, the risks can no longer be ignored. Knowing the extent of cloud services in use is a critical starting point.

But discovery is just the first step... beyond this implementing a programmatic way to enable organizations to take advantage of cloud services is essential.
Cloud Governance – Adoption Lifecycle

1. Discover
2. Cull
3. Consolidate
4. Control
5. Collaborate
6. Communicate

Right-Size → Right-Manage → Right-Trust
Cloud Governance – Adoption Lifecycle

Assurance for Cloud Operations Lifecycle

- **Discover**: Discovery of cloud services in enterprise
- **Cull**: Block/eliminate high-risk services
- **Consolidate**: Move unsanctioned clouds into sanctioned
- **Control**: Exert fullest control on scoped cloud
- **Collaborate**: Build guidelines/platform for adding new clouds
- **Communicate**: Fact-based communications to all stakeholders

**Right Size**

The discovery phase is the crucial first step which feeds directly into the development of a proper cloud assurance strategy that covers establishing the governance structure for adopting and managing cloud services.
Cloud Governance Outcomes

Confidence that systems are **secure**, data is **protected**, privacy issues have been dealt with, and ongoing risks are understood and will be well managed.

Confidence in the benefits that will accrue from the things that data can reveal about business operations.
Cloud Governance Outcomes

Confidence in the alignment of the organization’s cloud with business systems and services, including that systems have in place the right controls and strict monitoring to ensure they do what they’re supposed to do.

Confidence in the resilience of the organization’s overall IT and that all digital platforms will be available when required.
Cloud Governance Outcomes

Confidence that the organization’s cloud services will enable the enterprise to deliver a digital transformation program to move from legacy systems to modern systems involving cloud, mobile, social media, or other services and functions in ways that result in the expected benefits—on time and on budget and taking maximum advantage of the strengths of cloud services.
Cloud Governance Outcomes

Confidence based on deep understanding of the **nature and management of risk** in the organization’s cloud services lifecycle, which in turn increases trust in the organization, its operations, and its brand.
Because cloud services have implications across the entire enterprise, the lifecycle approach described here has steps business leaders must take to move their organizations toward secure and trustworthy cloud usage. Following are examples of business leader roles and main considerations throughout the lifecycle.
The CIO must lead the effort to discover the cloud services currently in use across the organization and their impact on operations.
CIO – Key Cloud Considerations

• How do I know employees are using sanctioned services?
• How do I make the people directing existing IT investments more cloud aware?
• Am I operating on the fewest possible cloud services to minimize risk yet utilizing the ones necessary for the organization’s success?
The CISO is ultimately responsible for blocking or eliminating high-risk cloud services.
CISO – Key Cloud Considerations

• What are the risks in the use of cloud services?
• Which cloud services do I need to block, and how do they rank by priority based on their risk to the enterprise?
• Is sensitive data passing through the cloud?
The CFO or COO will have an interest in moving unsanctioned cloud services into sanctioned ones and creating more cost efficient and more business efficient cloud use.
CFO/COO – Key Cloud Considerations

• Are our cloud services compliant with contract guidelines?
• Can I eliminate redundant use of cloud services and optimize cost and performance based on business needs?
• Can I get visibility into cloud risks that have an impact on my financial or operations reporting and build controls around them?
Role of Chief Audit Executive (CAE)

The CAE ensures that the right control framework, monitoring, and assurance are in place for cloud activities.
CAE – *Key Cloud Considerations*

- How do I comply with regulatory requirements?
- How do I assess whether cloud services are and remain within my audit scope?
- Do I need to deploy continuous and automated auditing capabilities for selected services?
Role of Business Line Executives

All BUSINESS LINE EXECUTIVES should reinforce cloud service guidelines and promote platforms for adding new cloud services.
Business Line Execs – Key Cloud Considerations

• Am I promoting the right cloud services that offer me the best time to market and effectively connect my business with my customers?
• How do I encourage my staff to work closely with IT in onboarding cloud services sustaining the enterprise’s security, data privacy and compliance objectives?
• Do I have a good sense of progress in terms of best practices and the operations metrics of how securely my organization is using cloud services?
Cloud Control

Strategy Formulation
- Goals
- Policies

Management Control
- Readiness assessment
- Communications & education
- Security process & procedures implementation
- Technology implementation

Task control
- Standards
- Metrics
- Performance analysis

CFO
CRO
CIO
CISO

Sourcing & contract management
Security program office
Risk management

Security program office
Security engineering
IT Operations
Knowledge Check

Multiple Choice

The person/role most responsible for blocking unauthorized cloud services is?

- CISO
- CAE
- CIO
- Batman
Sanity Check

**Let's implement cloud computing so I have something to talk about at the executive meeting.**

**Tell them we're evaluating it. That way neither of us needs to do any real work.**

**I like it when you do real work.**

**Sorry. I thought you were leading by example.**
CONCLUSION AND Q&A