

# Security in Cloud Computing

Edmond Kwan

*Director & Practice Leader*

*Security & Business Continuity*

*PricewaterhouseCoopers Consulting*

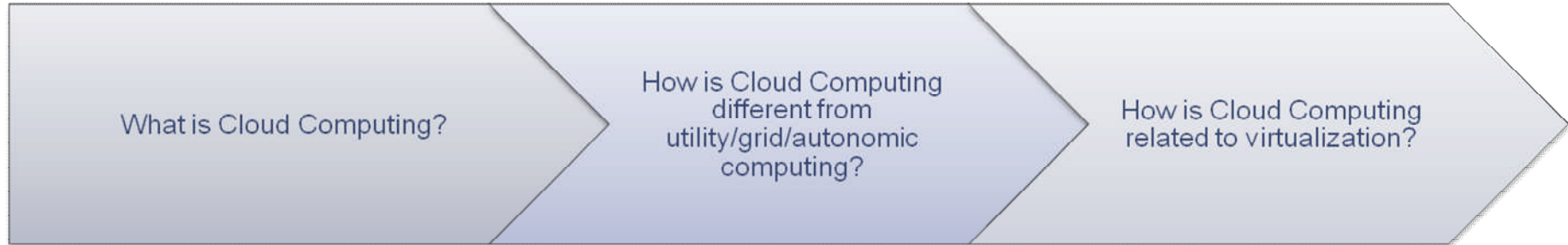
January 21, 2010



# Agenda

- Defining Cloud Computing ...
- Cloud Computing Candidates ...
- Security matters in the Cloud ...

# Defining Cloud Computing ...



# What is Cloud Computing?

- The term cloud is used as a metaphor for the Internet.
- No industry consensus on a definition of Cloud Computing.
- It is an evolution of technologies put together to meet the customers' needs for better and cheaper.
- It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet.
- Rely on the Internet to satisfy the computing needs of the users.

Multi-Tenant  
Platform-as-a-Service  
Scalability  
Virtualization  
Identity-as-a-Service  
Private Cloud  
Grid Computing  
Utility Computing  
Elasticity  
Web Services  
Service Model  
Online  
Computing Model  
Software-as-a-Service  
Hardware-as-a-Service  
Public Cloud  
Black Box  
On-Demand  
Service Oriented  
Business Model  
Security-as-a-Service

# Evolution of Cloud Computing

## Grid Computing

- Solving large problems with Parallel computing
- Made mainstream By Global Alliance



## Utility Computing

- Offering computing resources as a metered service
- Introduced in late 1990s



## SaaS Computing

- Network-based subscriptions to applications
- Gained momentum in 2001



## Cloud Computing

- Next-Generation Internet computing
- Next-Generation Data Centres



# Cloud Computing Defined – National Institute of Standards and Technology

“Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and three deployment models.” – May 2009, National Institute of Standards and Technology

<b>5 Key Characteristics</b>	<b>3 Deployment Models</b>	<b>3 Delivery Models</b>
1.On-demand self-service	1.Private Cloud	1.Software as a Service (SaaS)
2.Ubiquitous Network Access	2.Community Cloud	2.Platform as a Service (PaaS)
3.Location Independent Resource Pooling	3.Hybrid Cloud	3.Infrastructure as a Service (IaaS)
4.Rapid Elasticity		
5.Pay per Use		

## 5 Key Characteristics

1. **On Demand Self-Service** – Unilaterally provision resources as needed, automatically, without Human intervention
2. **Network Access Everywhere**– Accessible over common network protocols by varying devices and platforms (Accessing a set of “services”)
3. **Location Independent Resource Pooling** – Computing resources are pooled to serve all consumers (multi-tenant model), with physical and virtual resources dynamically assigned based on demand (“Resource Democratization”)
4. **Rapid Elasticity** – Scale up (or down) quickly and “infinitely”
5. **Pay Per Use** – Implement metering, pay by the minute/hour/Megabyte/Gigabyte

1. **Private/internal Cloud:** Infrastructure operated solely for organization only (can be onsite or offsite)
2. **Public/external Cloud:** Infrastructure is made available to general public or industry groups
3. **Hybrid Cloud:** Composition of two models

# 3 Delivery Models

*Defining Cloud Computing ...*

Cloud Computing services	Enabling technologies	Typical use	Examples
<b>Software as a Service (SaaS)</b> Applications that are provided and hosted in the Cloud, often built on other cloud services.	Server virtualisation SOA Web 2.0 Universal broadband	Enterprise applications Office productivity apps Web-based e-mail	Salesforce.com CRM Google Apps Hotmail, Gmail, Yahoo Mail
<b>Platform as a Service (PaaS)</b> Services that deliver a suite of solutions to allow online development and hosting of applications	SOA Open source development tools	Application design and development	Amazon Web Services Microsoft Azure Force.com Google App Engine
<b>Infrastructure as a Service (IaaS)</b> Services that deliver fundamental computing infrastructure: CPU cycles, storages etc.	Network, storage and server virtualisation Multi-core CPUs Cheaper networking bandwidth	Storage for off-site backup or archive Business or financial modelling farms	Amazon S3 Amazon EC2 GoGrid

Credit: docs.google.com

# So, what is Cloud Computing?

**Simple** definition:

“Cloud computing is a service offering that can scale up or down on-demand and has an utility cost model.”

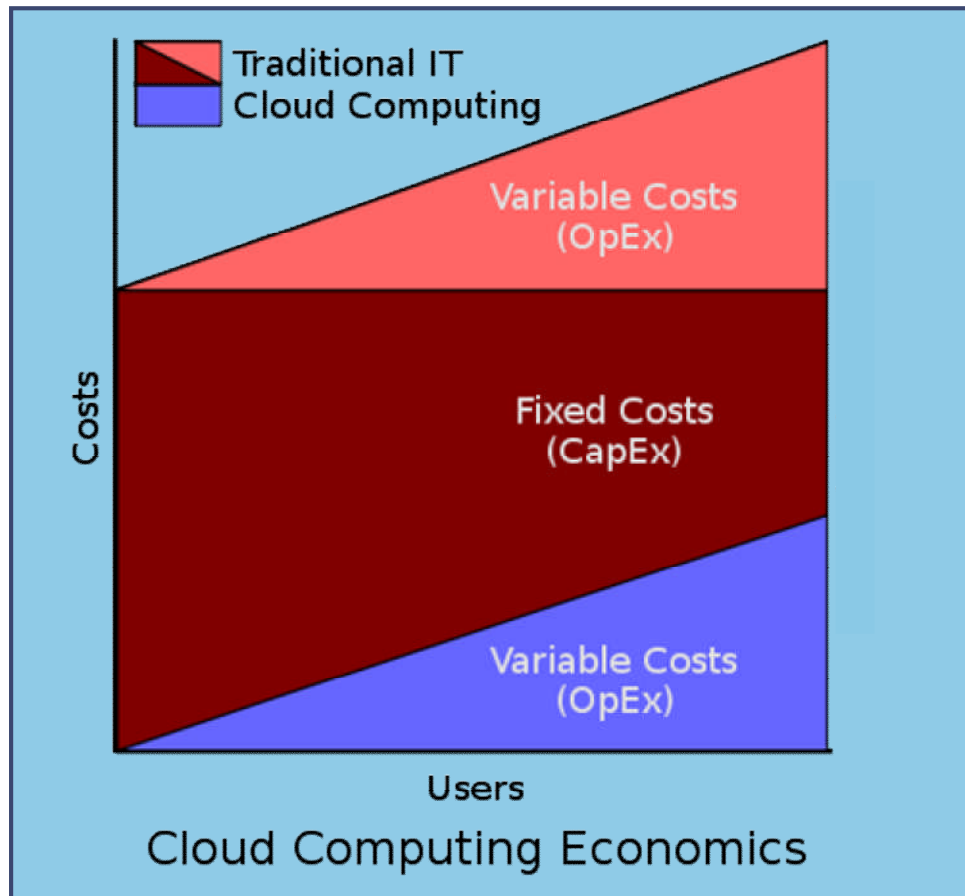
This elasticity of resources and granular usage measurement are what differentiates “Cloud” solutions from traditional hosted or managed services.

# Cloud Computing Candidates ...

*Cloud Computing Candidates ...*



# Advantages



- Users pay a provider only for what they use.
- Users can avoid capital expenditure (CapEx) on hardware, software, and services.
- Consumption is billed on a utility (e.g. resources consumed, like electricity) or subscription (e.g. time based, like a newspaper) basis with little or no upfront cost.

***Economics of cloud computing versus traditional IT, including capital expenditure (CapEx) and operational expenditure (OpEx)***

## Other Benefits of Cloud Computing

- Cost Savings/ Shared infrastructure and costs
- Flexibility/Agility/Scalability
- Centralization of Data/Applications (improves maintenance, sustainability, management, control)
- “Green” – idle computing resources
- Standardized and Hardened images - better resilience and defense against attacks
- Cloud Providers are Experts...

# Cloud Candidates

## Good Candidates

- Application performs well over request/response (stateless computing, bandwidth optimized, “web applications”)
- Packaged work/compute elements
- Highly fluctuating load patterns
- Non-sensitive data (at least for Public Cloud)
- Testing of new applications whose workload is unknown

## Poor Candidates

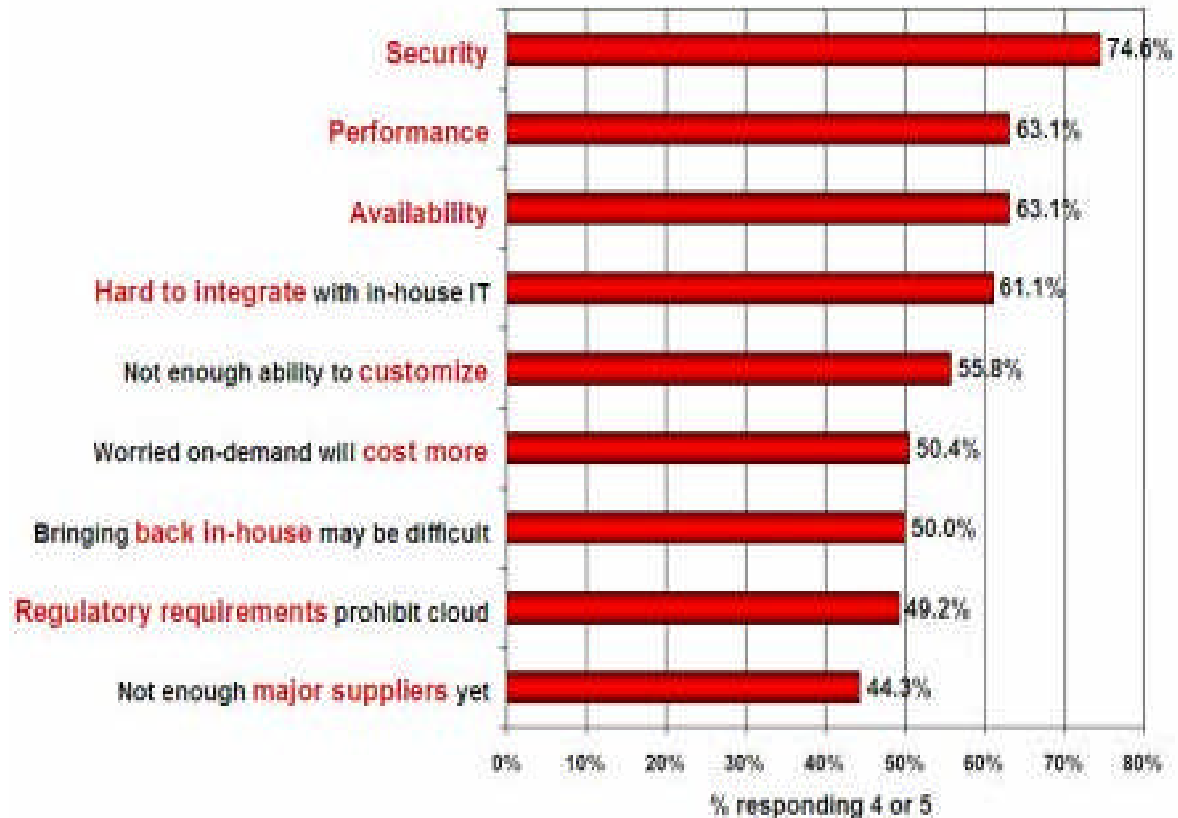
- Need to know where data is physically stored
- Data, applications and processes are tightly coupled
- Specialized Hardware required
- A higher degree of security is required (sensitive data)
- Existing enterprise architecture is in need of work

# Security matters in the Cloud ...



# Many challenges exist

In a key finding from a recent Cloud Computing Symposium survey, the attendees voted unanimously that Cloud Computing increases, not decreases the risk of data leakage

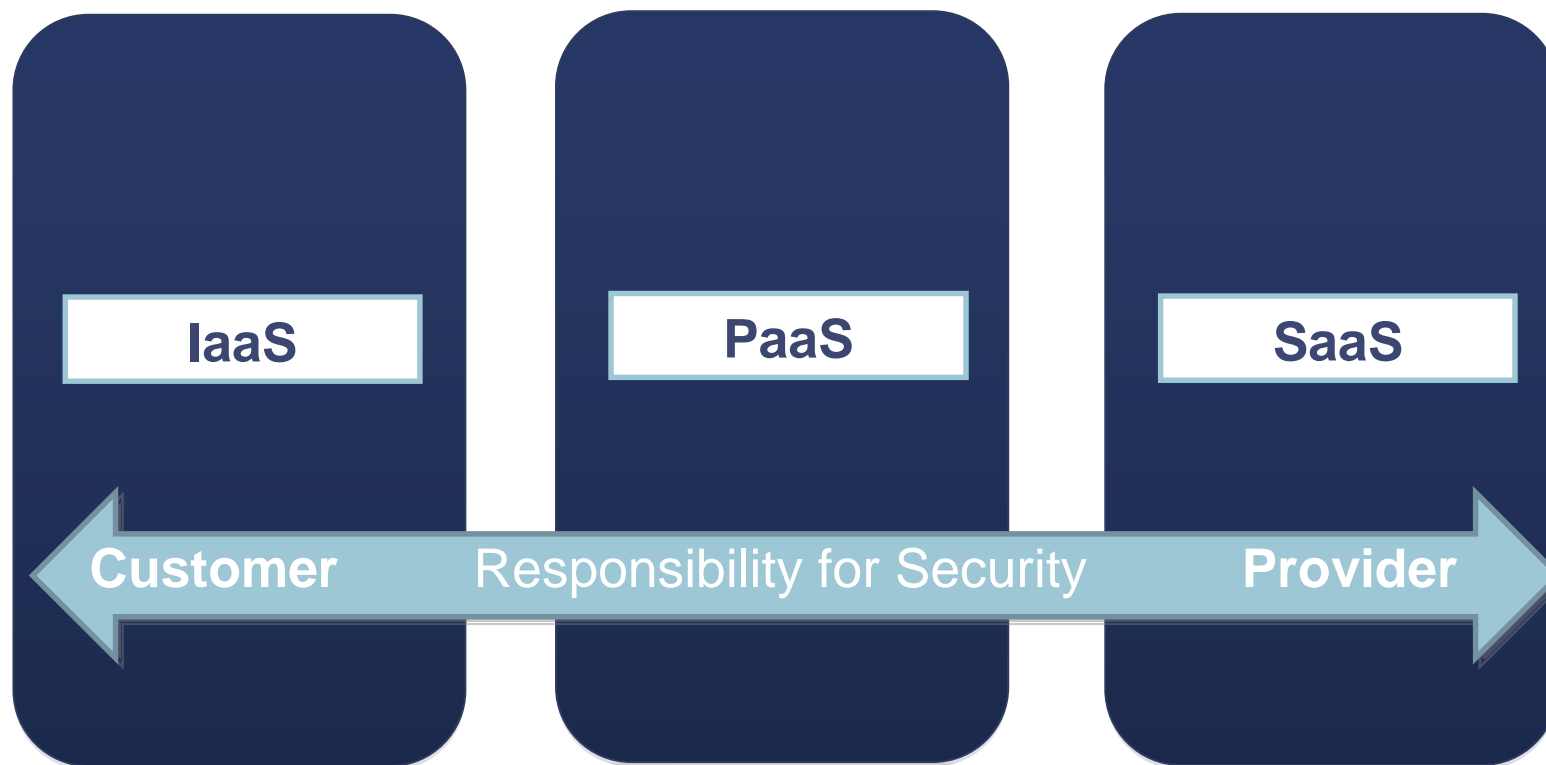


Ref. Forbes / IDC

# Information Security Governance in the Cloud



# Dynamic and Shifting Responsibilities for Security



# Cloud Risks – A complex matrix of overlapping risks

Issue	Risks				
	Regulatory	Legal	Operational	Security	Service
<b>Breach Notification</b>		X		X	X
<b>Denial of Service/Link Sharing/Web Application Vulnerabilities</b>			X	X	X
<b>Jurisdiction</b>		X			
<b>Acceptable Use</b>	X	X			
<b>Safe Harbour</b>	X	X			
<b>Data Segregation</b>	X	X	X		
<b>Subcontracting Services</b>	X				
<b>Business Continuity</b>			X		
<b>E-Discovery/Warrant/Forensics</b>	X	X	X		
<b>Threat &amp; Vulnerability Management</b>			X	X	X
<b>Right to Audit</b>	X				X
<b>Data Storage/Retention/Destruction</b>	X	X	X	X	
<b>Auditing &amp; Compliance</b>					
<b>Logging and Monitoring</b>	X		X	X	
<b>Incident Response &amp; Escalation</b>		X			X
<b>Data Encryption/Key Management</b>			X	X	
<b>User Access Management</b>				X	

# Regulatory Risks

- **Acceptable Use**
  - Is it acceptable for cloud providers to provide services in exchange for the right to mine your data? E.g. Google AdWords on Gmail?
- **Safe Harbour**
  - EU Data Protection Act requires personal data to be adequately protected when stored in “third countries”
  - Whose laws will take precedence in the event of a legal dispute? E.g. The application of the U.S. Patriot Act being served on a cloud storage provider?
- **Data Segregation**
  - How does one ensure data is fully segregated and not co-mingled/accessible?

# Regulatory Risks

- **Sub-Contracting Services**
  - Abstraction of “personnel” may result in untrustworthy or “conflicted” individuals having access to systems or data
- **E-Discovery/Warrant/Forensics**
  - What is the impact on customers data if a cloud “neighbour” is subject to a digital forensic investigation?
- **Data Storage/Retention/Destruction**
  - How does customer ensure all “copies” of data are adequately destroyed? Are off-site backups encrypted? Are they maintained in-line with corporate policy requirements (Data Classification)? Recovery Point Objectives?

- **Breach Notification**
  - Legal requirements to notify customers on breach of data maybe impacted by Cloud Provider policies, service levels, legal jurisdiction
- **Jurisdiction**
  - Which Legal jurisdiction applies should there be a legal dispute? What happens if data/servers are located in other jurisdictions? Who owns the data?

# Operational Risks

- **Denial of Service/Link Sharing/Web Application Vulnerabilities**
  - Attacks on Cloud Infrastructure, Cloud Vendors, Cloud Neighbours could have operational impacts on customer
  - Users of sites “trust” each other and share links (propagated by “social” worms)
  - Cross-Site Scripting/Cross-Site Request Forgery/SQL Injection
- **Threat and Vulnerability Management**
  - Exploited vulnerabilities can have serious operational impacts
  - Most Cloud Providers will terminate service contract if unauthorized scanning takes place
  - What happens if a customer scans cloud provider and knocks out service to other customers? How do you set scope? How do you comply with requirements to regularly perform scans?
- **Business Continuity**
  - Cloud Providers Disaster Recovery procedures could have impacts on customers? Do providers have the ability to prioritize recovery? How do customer’s plan and test BCP without provider participation? (hopefully robust, fault-tolerant nature of cloud reduces this risk)

- **Logging and Monitoring**
  - How robust (and complete) is Cloud Providers security logging and monitoring infrastructure and processes? Is access to underlying infrastructure logged? Auditable? Reviewed? Do customer controlled components contain adequate logging and monitoring? What about event correlation?
- **Data Encryption/Key Management**
  - Should all data in the Cloud be encrypted? Processing overhead? How robust is key management solution? What is the impact if a key is stolen? Does Cloud provider implement encryption? One key for all data? One key per customer?
- **User Access Management**
  - Affects both customer and provider
  - How does one ensure access rights are current and reflective of current business requirements? Management of “service accounts”?
  - How do you prevent Cloud Administrators from “seeing/copying” your data?

- **Right to Audit**
  - Difficult to negotiate, but a good practice for outsourced services to ensure compliance with information security policies, regulatory requirements (e.g. PCI)
  - Testing of key processes (e.g. Backup/Restore, Vulnerability Management, User Access Management etc.)
- **Incident Response and Escalation**
  - Does Cloud Provider have well designed incident response program? How and when does the customer get notified?
- **Change Management**
  - How does providers change management procedures integrate with customers? Testing? Risk Management?

# Cloud Computing Incidents Database

Date	Product	Provider	Severity	Incident Type	Affected	Comments
01/31/09	Google	Google	Critical	Outage	All Google's Internet search users affected	Lasted upto 1 hour
01/30/09	Ma.gnolia	Ma.gnolia	Critical	Data Loss	All	Both online and backup databases affected.
01/07/08	Salesforce.com	Salesforce.com	High	Outage	All	Affected all instances and supporting infrastructure
10/18/08	AWS Services	AWS	High	Security	All	Issue present since service launch
10/15/08	Gmail	Google	High	Outage	Unknown number of users	Lasted more than 24 hours
08/26/08	FlexiScale	FlexiScale	Critical	Outage	All	Full extended outage
07/09/08	.Mac	Apple	Info	Outage	All	Full outage (except mail) during upgrade to MobileMe 18:00-00:00
04/28/08	EC2	Amazon	Low	Outage	Small subset of instances	Result of a customer creating a large number of firewall rules and instances.
2007-2008	Carbonite	Carbonite	Critical	Data Loss		Customer data lost, storage vendor sued

[http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents\\_Database](http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents_Database)

# What help will clients need with Cloud Computing?

People	Process	Technology	Strategy	Structure
<ul style="list-style-type: none"><li>• Alignment of roles &amp; responsibilities to service delivery</li><li>• Staff training</li><li>• Reorganisation to adopt a service focus</li><li>• Update of success metrics</li><li>• Knowledge management</li></ul>	<ul style="list-style-type: none"><li>• Project planning</li><li>• Capacity planning and compute resource procurement</li><li>• Application prioritisation</li><li>• Developing &amp; managing service levels</li><li>• Vendor evaluation &amp; implementation</li><li>• Technology Adoption (Proof of Concept, Pilot, Deploy)</li></ul>	<ul style="list-style-type: none"><li>• Utility Computing architecture</li><li>• Identity management</li><li>• Data security</li><li>• Data management</li><li>• Systems management strategy</li><li>• Vendor evaluation &amp; implementation</li></ul>	<ul style="list-style-type: none"><li>• Defining a Cloud enabled IT strategy</li><li>• Updating financial models</li><li>• Updating standards and guidelines</li><li>• Building reference architectures for SaaS</li><li>• Updating the enterprise architecture</li></ul>	<ul style="list-style-type: none"><li>• Updating the governance model</li><li>• Defining and implementing controls</li><li>• Identifying audit procedures</li></ul>

**Cloud Computing is a disruptive technology which will transform how IT does business**

## Take away points

- Cloud Computing is a model that can help businesses cut cost, improve accessibility and resiliency.
- Cloud Services are in an infant state but quickly are moving towards mature, stable solutions.
- There are many security issues to consider in order to fully benefit from Cloud Computing.
- There is no standard “attestation” that has emerged for Cloud Computing - SAS 70 or ISO 27001 are starting points.

Thank U\*

© 2009 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, an Ontario limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity.