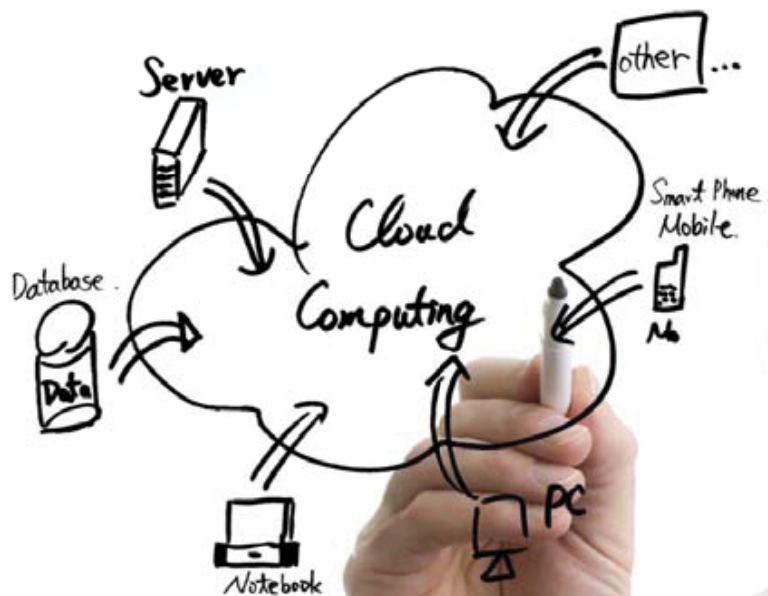# *How can we build trust in the cloud to drive business growth?*
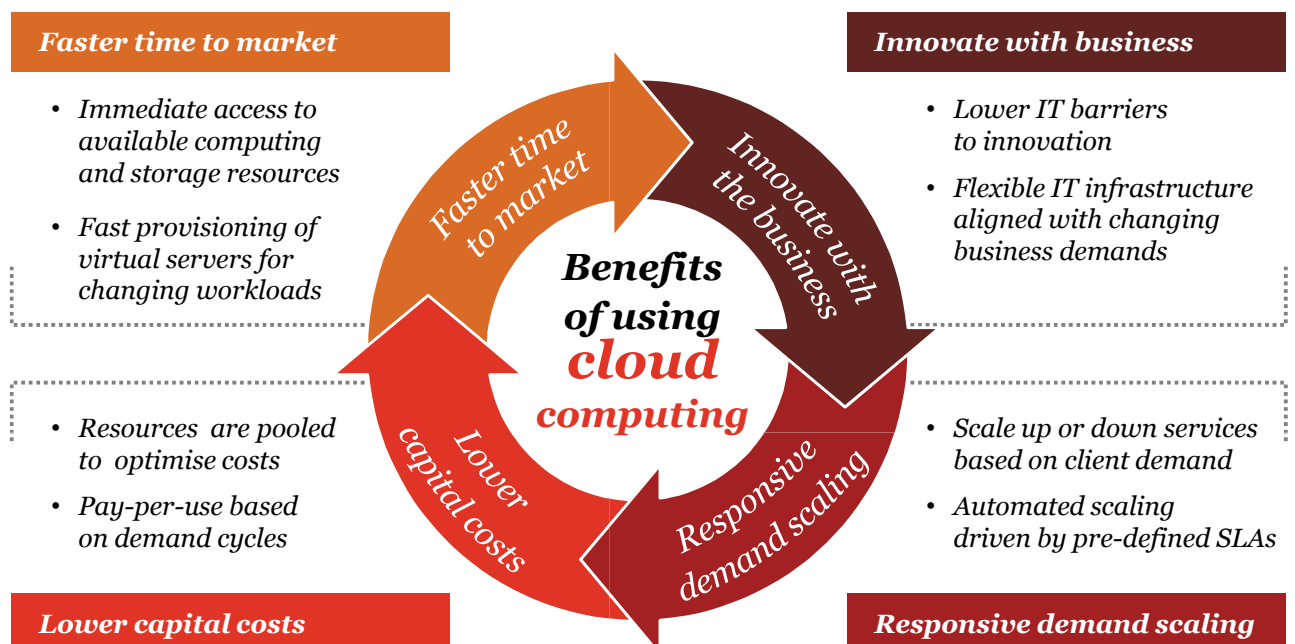
Cloud Assurance
March 2012

pwc

Background

Cloud computing is rapidly moving from hype to a must-have IT service model. It is transforming the way IT services are provided, consumed and managed.

Cloud computing has multifaceted definitions as it relates to the many types of IT users. For the line-of-business executive, cloud computing is a buyer-centric view of technology in which applications are available through rental rather than purchase or development.

For the CFO, the cloud offers an approach to consume the latest technologies in a pay-as- you-go model that delivers the cost benefits of variable pricing without a costly investment in hardware and software. And for the CIO, cloud computing provides an infrastructure and application model that can be rapidly provisioned and released to keep up with fluctuating demands.

Combine them, and it's clear that cloud computing holds enormous potential to help organisations drive growth in their business by achieving dramatic savings in operating costs, reducing complexity and increasing agility.

Faster time to market

- *Immediate access to available computing and storage resources*
- *Fast provisioning of virtual servers for changing workloads*

Innovate with business

- *Lower IT barriers to innovation*
- *Flexible IT infrastructure aligned with changing business demands*

Benefits of using cloud computing

Faster time to market

Innovate with the business

Lower capital costs

Responsive demand scaling

Lower capital costs

- *Resources are pooled to optimise costs*
- *Pay-per-use based on demand cycles*

Responsive demand scaling

- *Scale up or down services based on client demand*
- *Automated scaling driven by pre-defined SLAs*

What challenges are organisations facing?

Cloud computing promises to bring new levels of efficiency and agility, but internal and external stakeholders have many potential concerns when organisations consider any new technology that touches enterprise data and applications.

When adopting cloud services, our clients often ask us:

- What are the risks associated with cloud computing and how do we manage them?

- How will cloud computing impact our regulatory and compliance requirements?

- How do we maintain control and oversight over the cloud environment?

- Is moving to a cloud computing environment actually cost effective?

- What are the implications from an accounting and tax perspective?

- How will cloud computing impact on business continuity and disaster recovery planning?

The answer is not straightforward and needs to take into consideration the specific goals of the organisation and the nature of the cloud service and deployment model being adopted.

What challenges are organisations facing?

Cloud computing is resulting in a convergence of several traditional risks and also introducing additional risks to create unique challenges for organisations.

Examples of specific risks related to cloud computing include:

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

Termination arrangements
May not be adequately considered at the start.

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.

Data segregation
Inadequate segregation between different customers or regulated data in a cloud environment.

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

eDiscovery/ Investigation
May be challenging because data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and locations.

Legislation/Regulations
Difficult and potentially conflicting domestic and international legal and regulatory requirements (e.g. privacy, law enforcement access, encryption).

Political/cultural stability
Data may traverse or be stored in politically/ culturally unstable countries.

Taxation
May potentially incur international tax liabilities or miss out on tax opportunities due to differences in taxation laws between countries and jurisdictions.

Portability
Inability to migrate to or between cloud providers due to use of proprietary or incompatible technology or processes.

Scalability
Appears endless but may need advance planning with the provider with agreed service level agreements.

Long-term viability
The service provider may discontinue the cloud service, divest the cloud service or go into administration.

Contract
Inflexible and non-competitive contractual terms.

Licensing
Complicated licensing arrangement resulting in inadvertent breach of license agreement when deploying software and/hardware in a cloud environment.

Business continuity/ Disaster recovery
The recovery and continuity procedures may not meet organisational requirements resulting in significant financial loss or reputational damage.

Assurance
Inability to obtain sufficient assurance on controls within the cloud provider's environment.

Governance
Existing IT organisation and processes are not properly structured to govern new cloud services and providers.

Integration
Cloud service may not integrate with legacy systems and/or future systems.

Service levels
Service levels do not meet organisational requirements and the penalties for breaching service levels do not align with the business impact.

Customisation
Inability to customise cloud services to cater for organisational needs.

How can PwC help?

A successful adoption of cloud computing requires a new mindset, and new tools, to help ensure that risks are adequately managed. Without careful planning, the anticipated gains can easily be overshadowed by the perceived or actual risk exposures and prevent benefits from being realised.

PwC has helped several clients drive business growth by assisting them navigate and manage the risks associated with the cloud. Our Cloud Assurance services provide confidence to internal and external stakeholders (e.g. boards, audit committees, senior management, customers, service providers, regulators) that the risks related to cloud computing are adequately managed and the intended business benefits are being realised.

Cloud Assurance can help you:

- Assess and manage the technical, operational, financial, legal, regulatory, tax risks and opportunities associated with cloud adoption.

- Design and review the project framework to transition services to the cloud.

- Analyse the business case and costs to ensure business benefits are realistic and achievable.

- Design and review security and controls before, during, and after the move to the cloud.

- Design and review business continuity and disaster recovery procedures for cloud services.

- Provide third party assurance over cloud service providers' control environment (e.g. SSAE16 SOC2, ISO 27001, Cloud Security Alliance).

How can PwC help?

	Independent assurance to board and audit committee	Enabling operational efficiency and managing risks
Business challenge	• A large FMCG organisation planned to migrate their email to an outsourced cloud based service. • Management intended to gain cost savings and operational efficiencies, however was unsure whether they had adequately considered all the risks.	• A large government department planned to pilot the use of cloud computing services to replace their existing CRM and workflow management solutions, with the goal of providing staff with greater functionality and achieving operational efficiencies. • Management required assistance in identifying whether their risks related to pursuing a cloud-based solution were being effectively addressed.

PwC approach and results	• Through a series of risk workshops, we identified that:
	  – Management procured cloud services using their enterprise license arrangement with the vendor, but did not have a cloud specific contract.
	  – Workaround had to be designed for eDiscovery capability as it was not a standard feature.
	  – Impact on network performance and capacity needed more comprehensive planning.
	  – Data retention period did not align with organisational requirements.
	  – Dependencies and integration with other applications and business processes needed further analysis.
		• We conducted a series of risk workshops, where we identified:
		  – Risks related to trans-border data flows were not being adequately managed by the cloud services provider.
		  – There was a lack of clarity and visibility over assurance activities (e.g. testing of security and other IT controls) being conducted by the cloud provider.
		  – There were issues with continuity planning for the proposed new business processes.
		  – Inadequate consideration and documentation of integration between the cloud services and other systems and processes.

Value delivered	• Helped management with achieving their planned cost savings and operational efficiencies. • Provided confidence to the board and audit committee that risks are adequately managed.	• Helped management with achieving their planned goal of providing staff with greater functionality and achieving operational efficiencies, while still effectively managing their risks.

Some questions to ask when adopting cloud computing

- What guidelines are available to determine what should and should not be put into the cloud?

- How does migrating to a cloud environment affect our regulatory and compliance requirements?

- What are the implications of moving to a cloud computing environment from an accounting and tax perspective?

- Who owns the data in the cloud and who has the rights to use it?

- How can we restrict our data from flowing through certain countries and legal jurisdictions?

- What security measures are in place to protect our data in the cloud?

- How do we ensure our data is appropriately segregated from other cloud subscribers' data?

- What level of eDiscovery and investigation support is available in the cloud environment?

- How will migrating to the cloud environment affect our licensing arrangements for software and/or hardware?

- How do we get comfort over the long-term viability of the cloud service and the cloud provider?

- Who is liable if things go wrong and what are the remedies?

- What recovery and continuity procedures are available in the event of a loss of cloud service?

- How do we ensure that service levels and financial penalties are aligned to business impact and requirements?

- What tools, procedures and support are available to migrate between cloud providers?

- What monitoring and reporting mechanisms are available to maintain governance and oversight over the services migrated to the cloud?

- How can we change service providers or exit the contract without incurring additional costs or exposing ourselves to risks?

pwc.gr

Contacts:

Asterios Voulanas
Partner, Technology Risk Assurance
T: +30 210 6874714
E: stan.voulanas@gr.pwc.com