Deloitte.

Business Risks of Software in the Cloud

March 2, 2011

Andrew Murren
Deloitte & Touche, LLP
amurren@deloitte.com

Table of contents

Cloud Computing Overview

Definition of cloud computing

Cloud computing is a model for enabling 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 promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.

Essential Characteristics:

1. On-demand self-service.
2. Broad network access
3. Resource pooling
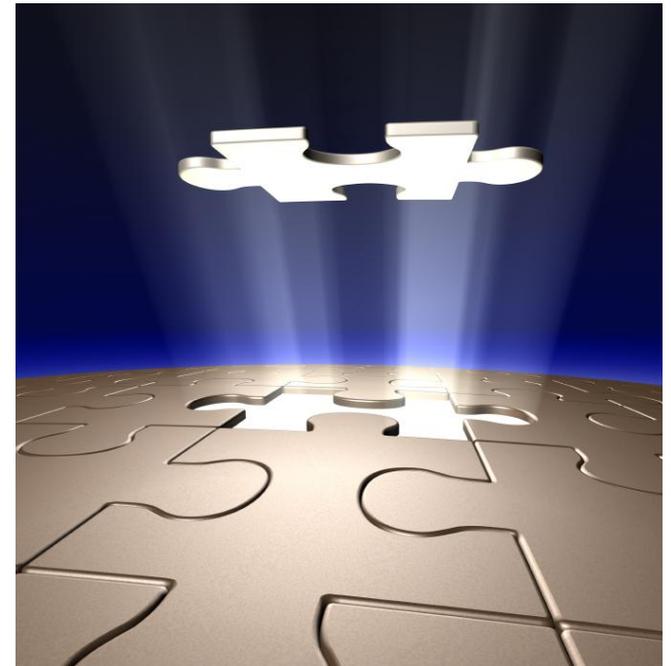4. Rapid elasticity
5. Measured Service

Deployment Models:

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

Service Models:

1. Cloud Software as a Service (SaaS)
2. Cloud Platform as a Service (PaaS)
3. Cloud Infrastructure as a Service (IaaS)

Source: http://csrc.nist.gov/groups/SNS/cloud-computing/

Cloud computing delivery models, based on their characteristics and purpose

Cloud computing technology is deployed in different ways, with varying internal or external ownership and technical architectures

Vendor cloud (External)	Cloud computing services from vendors that can be accessed across the Internet or a private network, using one or more data centers, shared among multiple customers, with varying degrees of data privacy control. Sometimes called "public" cloud computing.
Private cloud (Internal)	Computing architectures modeled after vendor clouds, yet built, managed, and used internally by an enterprise; uses a shared services model with variable usage of a common pool of virtualized computing resources. Data is controlled within the enterprise.
Hybrid cloud	A mix of vendor cloud services, internal cloud computing architectures, and classic IT infrastructure, forming a hybrid model that uses the best-of-breed technologies to meet specific needs.
Community cloud	Community clouds are used across organizations that have similar objectives and concerns, allowing for shared infrastructure and services. Community clouds can be deployed using any of the three methods outlined above, simplifying cross-functional IT governance.

Visualizing the differences
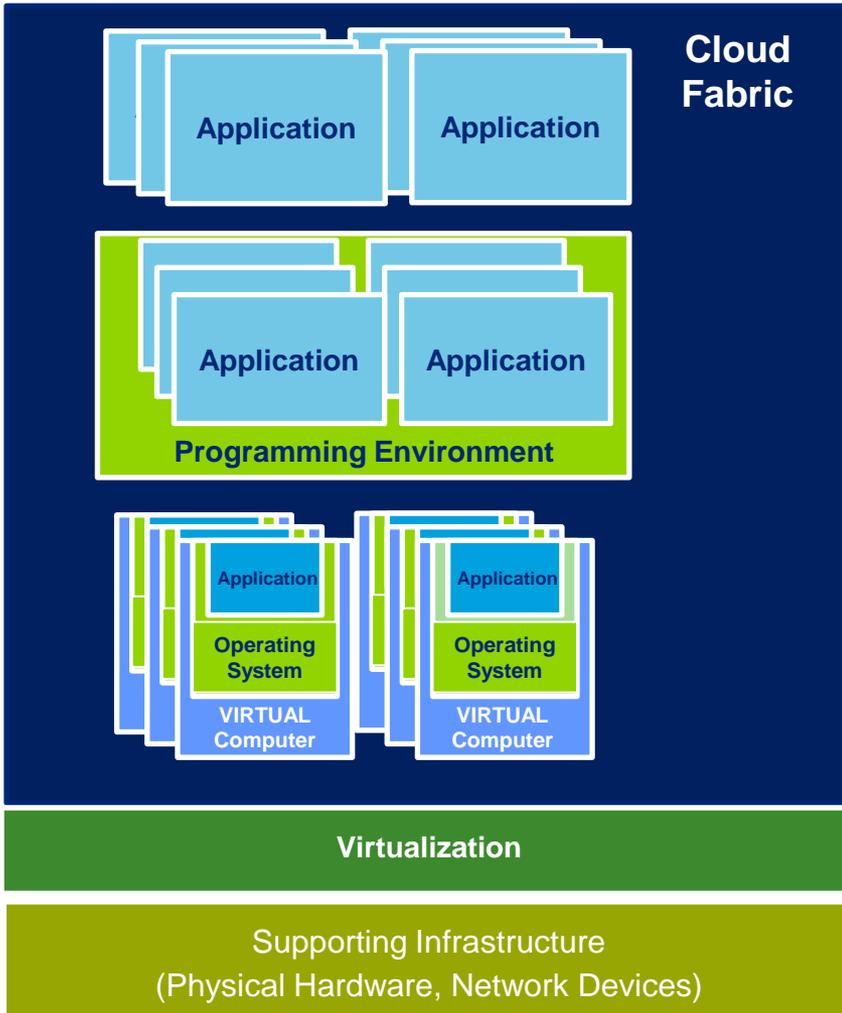
Software as a service (SaaS)

SaaS covers the range of application that are licensed for use as services provided to customers on demand typically across the Web.

Platform as a service (PaaS)

The PaaS model makes all of the facilities required to support the complete life cycle of building and delivering Web applications and services entirely available from the Internet.

Infrastructure as a service (IaaS)

IaaS is the delivery of computer infrastructure as a service. Rather than purchasing servers, software, data center space, or network equipment, clients instead buy those resources as a fully outsourced service.
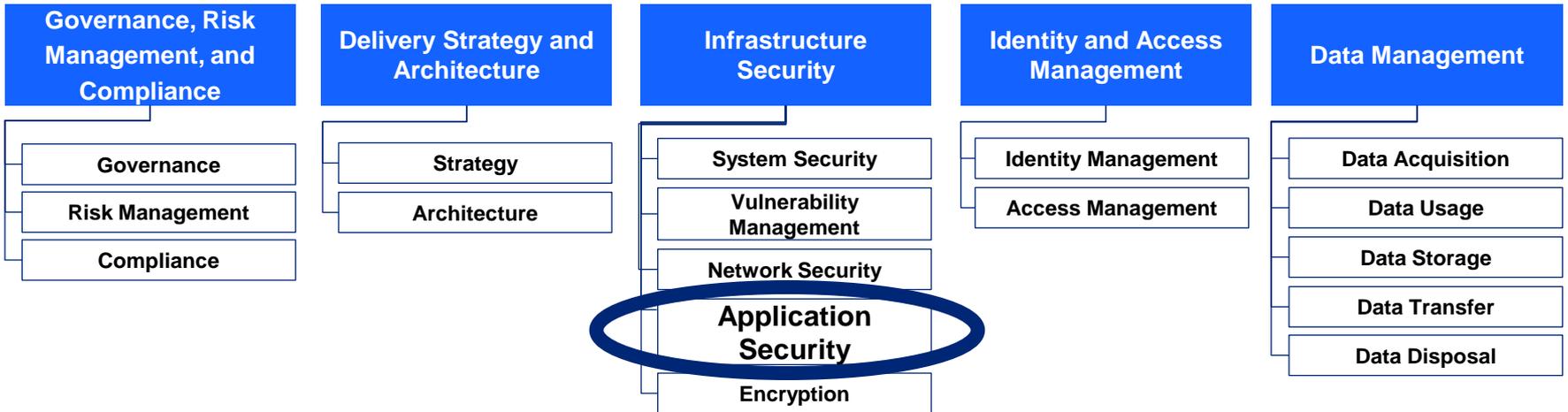
Virtual layer

Common IT Infrastructure

Risks in the Cloud

Deloitte's Cloud Computing Risk Intelligence Map

The Cloud Computing Risk Intelligence Map:

- Identifies significant risks that may be introduced by cloud computing
- Expands the risk discussion to the broad range of risks that need to be considered across the enterprise
- Spurs discussion about risk management topics, including risk identification, prioritization, measurement, and mitigation
- Facilitates the connection of risk management silos and identification of redundant efforts
- Can be customized for the client's individual cloud strategy and risk profile

Deloitte's Cloud Computing Risk Intelligence Map
Map categories and sub-categories

Governance, Risk Management, and Compliance
- Governance
- Risk Management
- Compliance

Delivery Strategy and Architecture
- Strategy
- Architecture

Infrastructure Security
- System Security
- Vulnerability Management
- Network Security
- Application Security
- Encryption

Identity and Access Management
- Identity Management
- Access Management

Data Management
- Data Acquisition
- Data Usage
- Data Storage
- Data Transfer
- Data Disposal

Business Resiliency And Availability
- Technology Resilience
- Cloud Provider Continuity
- Supply Chain Continuity

IT Operations
- Asset Management
- Project Management
- Change Management
- Incident Management
- Operations
- Physical & Environmental

Vendor Management
- Vendor Selection
- Contracting
- Monitoring
- Vendor Lock-in
- Resource Provisioning

Business Operations
- Human Resources
- Legal
- Finance
- Tax

IT Operations
Change Management

Updates to system and application configuration
- Who is responsible for what updates and within what time frame?
- Testing and validating configurations in constantly changing environments
- Ensuring only authorized people make approved changes to software and configurations
- Patching running systems and system templates

Pre and Post Deployment testing
- What environment to conduct testing in?
- Testing for correct functioning in constantly changing environment

Vendor Management
Vendor Selection

Cloud computing can push responsibility for software ownership and licensing issues to other organizations – but it can also disrupt your ability to operate.

Software developed in house by your cloud provider can run into patent or copyright problems, also putting you at risk.

Some questions to ask:

- Who is responsible for software licensing and ownership?
- What options are available if there is an issue with software we own or license?
- What can we do if parties we depend on have issues with the software they own, develop or license?
- How can we manage software costs in an elastic environment?

Infrastructure Security

Inability to independently test application security

Working with the Cloud provider
- Restrictions on continuous assessment and periodic security testing
- Coordinating software and configuration changes that may impact your systems

What is the security of the Cloud providers software
- What is the security posture of the software the Cloud provider is running?
- Does the cloud vendor securely configure their systems?
- What evidence of their security posture can they provide?

How will other Cloud users impact you
- Are other Cloud clients fully patched and up to date?
- What other software is running on systems?
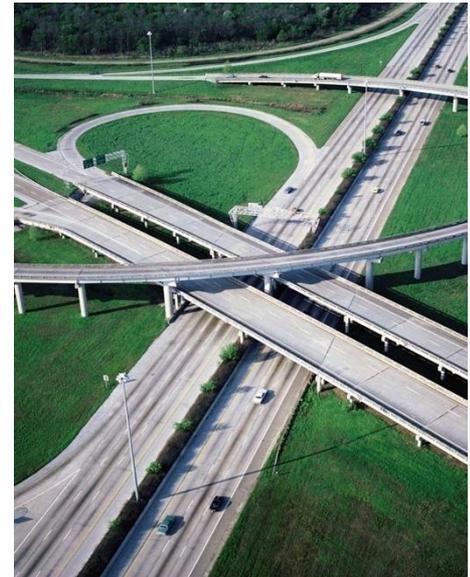
Questions?

Contact information

For additional information, please contact:	
Amry Junaideen Principal Deloitte & Touche LLP ajunaideen@deloitte.com +1 202 220 2664	**Irfan Saif** Principal Deloitte & Touche LLP isaif@deloitte.com +1 408 704 4109
Raymond Soriano Director Deloitte & Touche LLP rsoriano@deloitte.com +1 561 962 7735	**Andrew Murren** Manager Deloitte & Touche LLP amurren@deloitte.com +1 202 220 2121

Deloitte.