Assurance in the Cloud

Rob Zanella
Vice President
IT Compliance & Security
Certain information in this presentation may outline CA’s general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of April 2010 and is subject to change or withdrawal by CA at any time without notice. The development, release and timing of any features or functionality described in this presentation remain at CA’s sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.
CA Enterprise

13.4K+ Employees
137 Offices
45 Countries

- 13.4K+ Employees
- 137 Offices
- 45 Countries

Applications
> SAP (8) Modules
> 10 Packaged Applications
> 1,000 Custom Built Legacy Applications

Systems
> 1,300+ production servers: Linux, Unix, Windows
> 4 IBM mainframes: 20+ LPARS, 22K MIPS

Storage
> 890+ TB Array Storage

Network & Voice
> 40,000 Network Devices
> 1,500+ Voice & Data circuits worldwide
> 150+ phone systems
> 300+ routers & 465+ switches

Data Centers
> Islandia, NY. 10YRS
> Lisle, IL. 5 YRS
> Ditton Park, U.K.
> Hyderabad, INDIA
> Sydney, AUS

Security & Compliance
> 41 In Scope SOX Applications
> 559 Sox Controls
> 101 ITGCC
> 250 ACT (Application Controls Testing)
> 208 Access/SOD

Complexity
Manageability
80% Tier 1
VoIP
Risk

13.4K+ Employees
137 Offices
45 Countries
Agenda

- Defining the “Cloud”
- Benefits and Inhibitors
- Cloud Security
- Compliance Risks
What is 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.”
Essential Characteristics of Cloud Computing

- **On-demand self-service** - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each person’s provider.

- **Broad network access** - Capabilities are available over the network, and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- **Resource pooling** - The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

- **Rapid elasticity** - Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

- **Measured Service** - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
## Agreement on Definitions

<table>
<thead>
<tr>
<th>Service Delivery Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Use the provider’s application</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>User controls the applications</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>User controls the OS, CPU, DASD, and network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>Operated solely for one organization</td>
</tr>
<tr>
<td>Community Cloud</td>
<td>Shared by several orgs for one purpose</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>Available to the general public</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Composition of two or more clouds enabling data or application portability</td>
</tr>
</tbody>
</table>
Cloud Characteristics

**Essential Characteristics**

- Broad Network Access
- Elasticity
- Measured Service
- On-demand Self-Service

**Service Models**

- Platform as a Service
- Infrastructure as a Service
- Software as a Service

**Deployment Models**

- Private
- Hybrid
- Public
- Community

**Visual Model of Cloud Computing (source: NIST)**
Benefits

➢ Increase flexibility and agility
  ❖ Gain greater flexibility on architecture decisions and sourcing options
  ❖ Scale resources up and down as needed, maximizing capacity efficiency
  ❖ Accelerate time to value realization
  ❖ Significantly less time to start up and complete projects

➢ Reduce the amount of IT capital spending
  ❖ Use of “pay-as-you-go” subscriptions instead purchase/lease
  ❖ Move IT costs from capital expenditures to operating expenses

➢ Reallocation of staff resources
  ❖ As IT requirements are reduced, allocate resources to other value adding/decision support activities
Inhibitors to Adoption

“Security, risk management and compliance abilities were the number one decision factor customers considered when choosing a cloud service provider.” – Enterprise Management Assoc. 2010

- Lack of visibility or control
- Lack of privacy or security guarantees
- Security, risk, or compliance costs
- Control of data location/movement
- Vulnerability of immature technology
- Concern about cloud as attack target
- Poor responsibility definitions
- Lack of regulatory clarity
- Inability to prevent new risks
- Promises of security, compliance
- Business viability of providers
Cloud Security & Compliance Risks

- Data Protection and Privacy
  - Segregation of Data – from other customers
  - Location of Data – Regs require data to be held within local borders
  - Protection of Data at-rest – compromise in cloud
  - Protection of In-Transit data – encryption
  - Physical Backup of Data – method, privacy
  - Data Loss Prevention – monitorable?
  - Protection from Cloud Employees – Proper Admin rights
Cloud Security & Compliance Risks (cont.)

- Data Protection and Privacy
  - Vulnerability Management – scans, internal/external
  - Identity Management – integrate directly with my directories, support SSO, provision/de-provision
  - Physical Access – restricted access, background checks, any third-parties
  - Availability – SLA, capacity management, recourse
  - Application Security – testing, acceptance procedures (OWASP)
  - Incident Response – procedures, communication requirements
  - Liability – Intellectual property, end-of-service, SLA’s
Operational Compliance

1. Governance Framework
2. Certifiable
3. Defensible position with audit community (internal & external)
4. Predictable Risk Model
5. Operational Excellence
Cloud Management

- Only Classified data can be a candidate
  - Strategic – would cause harm if compromised: Internal Cloud Only
  - Confidential – employee records, sensitive customer info: Secure SaaS cloud most likely candidate
  - Corporate – normal corporate documents, data: External IaaS, PaaS, and SaaS can be considered

- Process Maturity
  - Must be at least documented and repeatable
  - Must have agreed upon Service Levels for consideration
Auditing the Cloud & Cloud Compliance

Scope the cloud computing environment
  - Which factors differ: public clouds vs. private clouds? (internal vs external)
  - Hard perimeter/soft interior no longer makes sense – change risk profile
    - Where does the cloud start and stop?

Modify risk assessment process to correctly capture risks
  - What is the population, universe
  - Sample selection in a highly dynamic environment
  - Consider peak/valley usage in selection

Audit trails
  - How do you “test” historical data if there was no audit trail? Need logs to evidence proper controls, monitoring

Abstract servers
  - How do you know that the server you’re auditing was the same server over time? Understand standard builds, config & change mgt.

Virtualization
  - Hypervisor configuration, Admin access

Audit’s New Role
  - Educate the audit committee, advise on risks to Business and IT
Questions...

Rob Zanella, CISA
VP, IT Compliance & Security
Email: robert.zanella@ca.com