Trust in, and value from, Cloud Computing

Presented by
Marc Vael
Chair of the Cloud Computing Task Force
Who started all this?

“What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing – they should be in a "cloud" somewhere. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud.”
Definition

Cloud computing = model for enabling convenient, on-demand broad network access to a shared pool of configurable computing resources that can be rapidly provisioned & released with minimal management effort or service provider interaction and with automatic measuring, controlling & optimization.

5 characteristics

3 service models

4 deployment models

NIST, Definition of Cloud Computing, October 2009
<table>
<thead>
<tr>
<th>Service Model</th>
<th>Definition</th>
<th>To Be Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.</td>
<td>Options to minimize the impact if the cloud provider has a service interruption</td>
</tr>
</tbody>
</table>
| Platform as a Service (PaaS) | Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider                                                | • Availability  
• Confidentiality  
• Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite)  
• Data ownership  
• Concerns around e-discovery                                                                 |
| Software as a Service (SaaS) | Capability to use the provider’s applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail). | • Who owns the applications?  
• Where do the applications reside?                                                                 |
Marketing packaging is becoming important...

- Storage as a Service
- Database as a Service
- Information as a Service
- Process as a Service
- Integration as a Service
- Security as a Service
- Management as a Service
- Testing as a Service...
<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Description of Cloud Infrastructure</th>
<th>To Be Considered</th>
</tr>
</thead>
</table>
| Private cloud       | • Operated solely for an organization  
                      • May be managed by the organization or a third party  
                      • May exist on-premise or off-premise | • Cloud services with minimum risk  
                      • May not provide the scalability and agility of public cloud services |
| Community cloud     | • Shared by several organizations  
                      • Supports a specific community that has shared mission or interest.  
                      • May be managed by the organizations or a third party  
                      • May reside on-premise or off-premise | • Same as private cloud, plus:  
                      • Data may be stored with the data of competitors. |
| Public cloud        | • Made available to the general public or a large industry group  
                      • Owned by an organization selling cloud services | • Same as community cloud, plus:  
                      • Data may be stored in unknown locations and may not be easily retrievable. |
| Hybrid cloud        | A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) | • Aggregate risk of merging different deployment models  
                      • Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type. |
Outsource
61% of respondents feel big data will fundamentally change the way their business works.
Legacy

- Centralized/monolithic computing layer
- Computer networking limited
- Relational databases
- FC SAN/NAS
- Disks/Tape (memory scarce/expensive)
- Proprietary/closed vendors
- Enterprise-scale

Cloud

- Distributed computing layer (virtual machines, Map Reduce, networked commodity servers)
- High speed networking is pervasive
- Non-relational/"no sql" data stores
- Distributed file systems
- Flash/SSD (high performance and abundant)
- Open platforms
- Internet/cloud scale
Trust creates the opportunity for Value

Value is based on an expectation of Trust

Trust:
1. Confidentiality
2. Privacy
3. Integrity
4. Availability
5. Compliance
6. Licensing
7. Reliability
8. Monitoring
9. Integration
10. Network centric

Value:
1. Lower upfront investments
2. More OPEX than CAPEX
3. On demand Convenience
4. Dynamic scalability
5. Optimized resource usage
6. Flexibility
7. Business control over IT solutions
8. Centralized data (sort of)
9. Shorter development cycle
10. Faster implementation
11. Logging & Monitoring
12. Green IT
Cloud Ready?

- When the processes, applications and data are largely independent
- When the points of integration are well defined
- When a lower level of security will work just fine
- When the core internal enterprise architecture is healthy
- When the Web is the desired platform
- When cost is an issue
- When the applications are new

*Used with permission from David Linthicum*
Which are the two most important risks of cloud computing?

<table>
<thead>
<tr>
<th>Risk</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy</td>
<td>49.3%</td>
</tr>
<tr>
<td>Data security</td>
<td>41.3%</td>
</tr>
<tr>
<td>Availability</td>
<td>21.9%</td>
</tr>
<tr>
<td>Data ownership</td>
<td>21.3%</td>
</tr>
<tr>
<td>Data location</td>
<td>14.6%</td>
</tr>
<tr>
<td>Data SLA's</td>
<td>12%</td>
</tr>
<tr>
<td>Lock-in</td>
<td>11.7%</td>
</tr>
<tr>
<td>Data integrity</td>
<td>10.1%</td>
</tr>
<tr>
<td>Situation service provider (merger-acquisition-broker)</td>
<td>5.6%</td>
</tr>
<tr>
<td>Data encryption</td>
<td>4.8%</td>
</tr>
<tr>
<td>Other</td>
<td>1.6%</td>
</tr>
<tr>
<td>Don't know</td>
<td>1.3%</td>
</tr>
</tbody>
</table>
What’s The Primary Reason Your Company Won’t Use Public Cloud Services?

- Fear of unauthorized access to or leak of our proprietary information: 28%
- Fear of unauthorized access to or leak of our customers’ information: 17%
- Features and general maturity of technology: 12%
- Security defects in the technology itself: 8%
- Unpredictable costs: 6%
- Business viability of provider; risk company will fail: 5%
- Vendor lock-in: 5%
- Application or system performance: 4%
- Other: 15%

Data: InformationWeek Analytics Cloud GRC Survey of 208 business technology professionals with no plans to use cloud computing
Anti-Cloud Computing

Who played the most significant role opposing cloud computing?

- CIO or CTO: 32%
- Executive corporate management: 17%
- Other IT management: 17%
- IT staff: 16%
- Other: 11%
- No one: 1%
- Don’t know: 5%

Data: *InformationWeek Analytics* survey of 114 business tech pros at companies not evaluating or using cloud computing, April 2010.
About Cloutage

Cloutage exists to empower organizations by providing cloud security knowledge and resources so that they may properly assess information security risks. The project aims to document known and reported incidents with cloud services while also providing a one-stop shop for cloud security news and resources. For any questions about this site or the data contained within the site, please contact stewards@cloutage.org.

Cloutage Blog

Open Security Foundation Announces New Advisory Board
by Jake Kouns, 2010-09-08

As security vulnerabilities and data loss incidents become a regular occurrence, the Open Security Foundation has grown from supporting a single project in 2004 to a leading provider of filtering through security information and providing notifications and aggregation for data for data loss and cloud security incidents.

The Open Security Foundation has evolved into one of the most utilized resources in providing security information, and as a 501c3 non-profit organization relies heavily on public contributions, volunteer effort and corporate sponsorships.

The growing demand for information to provide proper risk management has led to additional projects and now the introduction of an advisory board consisting of industry professionals to lend their expertise in areas to keep OSF moving in a positive direction and to be the first line of access to all that require their service.

Open Security Foundation CEO and founder Jake Kouns stated, “This is a very important step in shaping the future of the Open Security Foundation.”

Latest Cloud Incidents

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Organization</th>
<th>What Happened?</th>
</tr>
</thead>
<tbody>
<tr>
<td>outage</td>
<td>2011-04-21</td>
<td>Amazon Web Services</td>
<td>Companies left staggering or totally knocked out because of server problems in the Amazon datacenter</td>
</tr>
<tr>
<td>outage</td>
<td>2011-04-21</td>
<td>Sony</td>
<td>PlayStation Network outages</td>
</tr>
<tr>
<td>outage</td>
<td>2011-03-25</td>
<td>Twitter, Inc.</td>
<td>Twitter Experiences Delays in Delivering to Facebook and SMS</td>
</tr>
<tr>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku</td>
<td>Heroku Users Experience HTTP 503 Errors</td>
</tr>
<tr>
<td>outage</td>
<td>2011-03-25</td>
<td>Twitter, Inc.</td>
<td>Twitter Experiences Tweet Delivery Delay</td>
</tr>
<tr>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku</td>
<td>Heroku Shared Database Experienced Hardware Failure</td>
</tr>
<tr>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku</td>
<td>Heroku Users Unable to Provision New Dedicated Databases</td>
</tr>
<tr>
<td>hack</td>
<td>2011-03-24</td>
<td>Expedia</td>
<td>TripAdvisor Member Data Stolen in Possible SQL Injection Attack</td>
</tr>
</tbody>
</table>
Keep 15 basic outsourcing “lessons learned” in mind:

1. Psychological impact
2. IT governance model
3. Integration with internal IT systems
4. Network connectivity / bandwidth
5. Data location
6. Shared tenancy
7. Vendor lock-in
8. Cloud Service Provider stability, reliability and viability
9. Service portability
10. Legal & regulatory compliance requirements (including licensing, contractual arrangements, record protection for forensic audit)
11. Information security management (including IAM)
12. Incident response & crisis management
14. Data ownership, archiving & removal
15. (Right to) Audit (pentest, screening, monitoring, …)
Cloud Computing Compliance “Tools”

- ISO 27002  Information Security Mgt
- ISO 38500  Corporate Governance Enterprise IT
- ISO 20000  IT Service Mgt
- ISO 15489  Records Mgt
- ISACA CobiT  IT Governance & Audit
- ISACA Val IT  IT Investment Governance
- ISACA Risk IT  IT Risk Mgt
- ISACA BMIS  Business Information Security Mgt
- BS 25999  Business continuity
- BS 25777  IT continuity
- CSA  GRC stack
Your cloud computing solution is as strong ...

... as its weakest link
Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

Cloud computing is an emerging technology that may help enterprises meet the increased requirements of lower total cost of ownership (TCO), higher return on investment (ROI), increased efficiency, dynamic provisioning and utility-like pay-as-you-go services. However, many IT professionals are citing the increased risks associated with trusting information assets to the cloud as something that must be clearly understood and managed by relevant stakeholders. In addition to the white paper, information on cloud computing, and understanding how a cloud initiative could align with a business, is provided by the following resources:

The book issued in July 2011 contains the audit program:

- IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

Join the discussion in the Knowledge Center.

- Cloud Computing

Listen to the Cloud Webcast presented by Peet Rapp and Phil Lageschulte

- Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives

Additional Information on Cloud Computing:
Cloud Computing Management Audit/Assurance Program

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. ISACA has commissioned audit/assurance programs to be developed for use by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF section 2200—General Standards. The audit/assurance programs are part of ITAF section 4000—IT Assurance Tools and Techniques.

Objective—The cloud computing audit/assurance review will:

- Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider’s internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provide audit stakeholders with an assessment of the quality of and their ability to rely upon the service provider’s attestations regarding internal controls.

It is not designed to replace or focus upon audits that provide assurance of specific application processes and excludes assurance of an application’s functionality and suitability.

Scope—The review will focus on:

- The governance affecting cloud computing
- The contractual compliance between the service provider and customer
- Control issues specific to cloud computing

IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and/or necessary subject matter expertise to adequately review the work performed.
Cloud Computing

Collaborate, contribute, consume and create knowledge around Cloud Computing. Click "Join Now" to become a full contributing member of this topic.

You must be a member of ISACA to join this group. Join now!

Community Leader

Marc Vael
Title: Chief Audit Executive

Ramses
Title: Security Strategist & Evangelist

Recent Discussions
- What is Cloud Maturity?. Posted by Ron Hale Ph.D. CISM.
- Why Banks Fear the Cloud?. Posted by Bassil Mohammad.
- Cloud Computing approach. Posted by Marc Vael.

More »
References: Relevant Cloud Computing websites

- www.cloudsecurityalliance.org/
- csrg.nist.gov/groups/SNS/cloud-computing/
- opencloudconsortium.org/
- www.opencloudmanifesto.org/
- www.cloud-standards.org/wiki/
- en.wikipedia.org/wiki/Cloud_computing
- searchcloudcomputing.techtarget.com/
- cloudcomputing.sys-con.com/
- cloudsecurity.org/
- www.cloudaudit.org/
- www.isaca.org/cloud
IT CONTROL OBJECTIVES 

for CLOUD COMPUTING: 

CONTROLS AND ASSURANCE IN THE CLOUD
Contact information

Marc Vael
CISA, CISM, CISSP, CGEIT, ITIL Service Manager, Prince2
Director Knowledge Board
Chairman Cloud Computing Task Force

http://www.isaca.org/cloud

marc@vael.net
http://www.linkedin.com/in/marcvael
http://twitter.com/marcvael
The Leadership Forum for Business and IT Professionals

25-27 June 2012
San Francisco, California, USA
www.isaca.org/insights