Cloud Computing

Cloud Computing
An insight in the Governance & Security aspects

Marc Vael

AGENDA

• Introduction
• Security
• Governance
• Risks
• Compliance
• Recommendations
• References
Cloud Computing

Peter Hinsen, The New Normal, 2010
Cloud Computing

Peter Hinssen, The New Normal, 2010

Which SaaS Vendors Do You Use?

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salesforce.com</td>
<td>41%</td>
</tr>
<tr>
<td>Google</td>
<td>28%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>26%</td>
</tr>
<tr>
<td>Oracle</td>
<td>26%</td>
</tr>
</tbody>
</table>

Data: InformationWeek Analytics SaaS Survey of 131 business technology professionals at companies using SaaS, November 2009

What Are Your SaaS Plans?

<table>
<thead>
<tr>
<th>Application</th>
<th>Planned delivery within 18 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>50%</td>
</tr>
<tr>
<td>HR and recruiting</td>
<td>38%</td>
</tr>
<tr>
<td>Web presence</td>
<td>33%</td>
</tr>
<tr>
<td>E-mail</td>
<td>31%</td>
</tr>
</tbody>
</table>

Data: InformationWeek Analytics SaaS Survey of 131 business technology professionals at companies using SaaS, November 2009

Marc Vael
Across
ISACA Belgium
May 2010
Cloud Computing

AGENDA

- Introduction
- Security
- Governance
- Risks
- Compliance
- Recommendations
- References
Cloud Computing

Analyzing Cloud Computing Security

• Cloud computing = outsourcing on steroids
  ‣ Security elements related to outsourcing!

Considerations in Cloud Computing Service Models

<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). |

### Considerations in Cloud Computing Deployment Models

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Description of Cloud Infrastructure</th>
<th>To Be Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud</td>
<td>Operated solely for an organization</td>
<td>Cloud services with minimum risk</td>
</tr>
<tr>
<td></td>
<td>May be managed by the organization or a third party</td>
<td>May not provide the scalability and agility of public cloud services</td>
</tr>
<tr>
<td></td>
<td>May exist on-premise or off-premise</td>
<td></td>
</tr>
<tr>
<td>Community cloud</td>
<td>Shared by several organizations</td>
<td>Same as private cloud, plus:</td>
</tr>
<tr>
<td></td>
<td>Supports a specific community that has shared mission or interest.</td>
<td>Data may be stored with the data of competitors.</td>
</tr>
<tr>
<td></td>
<td>May be managed by the organizations or a third party</td>
<td></td>
</tr>
<tr>
<td></td>
<td>May reside on-premise or off-premise</td>
<td></td>
</tr>
<tr>
<td>Public cloud</td>
<td>Made available to the general public or a large industry group</td>
<td>Same as community cloud, plus:</td>
</tr>
<tr>
<td></td>
<td>Owned by an organization selling cloud services</td>
<td>Data may be stored in unknown locations and may not be easily retrievable.</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>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)</td>
<td>Aggregate risk of merging different deployment models</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.</td>
</tr>
</tbody>
</table>

**8 General Cloud Computing Security Advantages**

1. **Benefits of scale**
2. **Provider market differentiator**
3. **Standardized interfaces for Managed Security Services**
4. **Rapid & Smart scaling of security resources**
5. **Security audit & evidence gathering**
6. **Timely & effective & efficient updates & defaults**
7. **Security risk management**
8. **Resource concentration benefits**
Cloud Computing

14 Specific Cloud Computing Security Challenges

1. Migrating PII & sensitive data to the cloud
   › EU Data Protection Directive & U.S. Safe Harbor program
   › Exposure of data to foreign government & data subpoenas
   › Data retention & records management issues
   › Privacy Impact Assessments (PIA)

2. Identity & Access Management

3. Multi-tenancy

4. Logging & Monitoring

5. Data ownership / custodianship

6. Quality of Service guarantees

7. Securing hypervisors (BluePill)

8. Attracting hackers (high value target)

9. Security of virtual OS in the cloud

10. BCP / DRP

11. Data encryption & key management
   › Encrypting access to cloud resource control interface
   › Encrypting administrative access to OS instances
   › Encrypting access to applications
   › Encrypting application data at rest

12. Public cloud vs. Internal cloud security

13. Lack of public SaaS version control

14. Using SLAs to obtain cloud security
   › Suggested requirements for cloud SLAs
   › Issues with cloud forensics & e-discovery
Cloud Computing

AGENDA

- Introduction
- Security
- Governance
- Risks
- Compliance
- Recommendations
- References

5 Key Governance issues around Cloud Computing

- **Transparency**: providers must demonstrate existence of effective & robust security controls, assuring customers their information is properly secured against unauthorized access, change & destruction.
  - How much transparency is enough?
  - What needs to be transparent?
  - Will transparency aid malefactors?
  - Which employees (of the provider) have access to customer information?
  - Is Segregation of Duties (SoD) between provider employees maintained?
  - How are different customers’ information segregated?
  - What controls are in place to prevent, detect and react to security breaches?
5 Key Governance issues around Cloud Computing

• **Compliance**: concerns with cloud computing that data may not be stored in 1 place & may not be easily retrievable.
  
  ‣ Ensure that, if data are demanded by authorities, data can be provided without compromising other information.
  
  ‣ Audits completed by legal, standard and regulatory authorities themselves demonstrate that there can be plenty of overreach in such seizures.
  
  ‣ When using cloud services, there is no guarantee that an enterprise can get its information when needed, and some providers are even reserving the right to withhold information from authorities.

5 Key Governance issues around Cloud Computing

• **Trans-border information flow**: When information can be stored anywhere in the cloud, the physical location of the information can become an issue.
  
  ‣ Physical location dictates jurisdiction and legal obligation.
  
  ‣ Country laws governing personally identifiable information (PII) vary greatly.
  
  ‣ What is allowed in one country can be a violation in another.
5 Key Governance issues around Cloud Computing

- **Privacy**: imperative for providers to prove to customers that privacy controls are in place & demonstrate ability to prevent, detect and react to security breaches in a timely manner.
  - Information & reporting lines of communication need to be in place & agreed on before service provisioning commences.
  - Communication channels should be tested periodically during operations.

- **Certification**: providers will need to provide assurance to their customers that they are doing the “right” things.
  - Independent assurance from third-party audits and/or service auditor reports should be a vital part of any cloud computing program.
Cloud Computing

AGENDA

- Introduction
- Security
- Governance
- Risks
- Compliance
- Recommendations
- References

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

1 = not significant, 5 = very significant

<table>
<thead>
<tr>
<th>Challenge</th>
<th>% Responding 4 or 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>74.0%</td>
</tr>
<tr>
<td>Performance</td>
<td>63.1%</td>
</tr>
<tr>
<td>Availability</td>
<td>63.1%</td>
</tr>
<tr>
<td>Hard to integrate with in-house IT</td>
<td>61.1%</td>
</tr>
<tr>
<td>Not enough ability to customize</td>
<td>55.6%</td>
</tr>
<tr>
<td>Worried on-demand will cost more</td>
<td>50.4%</td>
</tr>
<tr>
<td>Bringing back in-house may be difficult</td>
<td>50.0%</td>
</tr>
<tr>
<td>Regulatory requirements prohibit cloud</td>
<td>49.2%</td>
</tr>
<tr>
<td>Not enough major suppliers yet</td>
<td>44.3%</td>
</tr>
</tbody>
</table>

Source: IDC Enterprise Panel, August 2008, n=244
Cloud Computing

Vulnerabilities on Cloud Computing

Authentication, Authorization, Accounting
User (de)provisioning
Remote access to mgt interface
Hypervisor
Lack of resource isolation
Lack of reputational isolation
Communication encryption
Lack of encryption of archives / data in transit
Impossibility to process data in encrypted form
Poor key mgt procedures
Random number generation issue for encryption key generation
Lack of standard technologies
No source escrow agreement
Inaccurate modeling of resource usage
No control on vulnerability assessment process
Possible internal network probing

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

Vulnerabilities on Cloud Computing

- Possible check on co-residence
- Lack of forensic readiness
- Sensitive media sanitization
- Contractual obligations
- Cross cloud applications creating hidden dependency
- Conflicting SLA clauses
- Excessive SLA clauses
- No audit / certification available
- Certification scheme not adapted to cloud infrastructure
- Inadequate resource provisioning / investment in infrastructure
- No policies for resource capping/limits
- Data storage in multiple jurisdictions
- Lack of info on jurisdictions
- Lack of completeness & transparency in terms of use
- ...

Generic vulnerabilities related to Cloud Computing

- Lack of security awareness
- Lack of vetting process
- Unclear roles & responsibilities
- Poor enforcement of role definitions
- No need-to-know principle applied
- Inadequate physical security procedures
- Misconfiguration
- System / OS vulnerabilities
- Untrusted software
- No/Poor BCP/DRP
- No/Incomplete asset inventory
- No/Unclear asset ownership
- Poor identification of project requirements
- Poor provider selection
- Lack of supplier redundancy
- Poor patch mgmt
- ...

Marc Vael
Across

ISACA Belgium
May 2010
Cloud Computing

7 top threats on Cloud Computing

1. Abuse & inappropriate use of cloud computing
2. Insecure interfaces & APIs
3. Malicious insiders
4. Shared technology issues
5. Data loss / leakage
6. Account / Service hijacking
7. Unknown risk profile

CSA, Top Threats to Cloud Computing v1, March 2010

Cloud Computing Risk Areas

Policy & Organizational risks

1. Provider Lock in*
2. Loss of Governance*
3. Compliance challenges*
4. Loss of business reputation due to co-tenant activities
5. Cloud service termination/failure
6. Cloud provider acquisition
7. Supply Chain failure
8. SLA challenges
# Cloud Computing

Cloud Computing Risk Areas

## Technical risks
1. Isolation failure*
2. Malicious insider at cloud provider*
3. Management interface compromise*
4. Insecure/ineffective data deletion*
5. Malicious scans
6. Resource exhaustion
7. Intercepting data in transit
8. Data leakage
9. DDoS
10. Loss of encryption keys
11. Compromise service engine
12. Conflicts customer procedures vs cloud procedures

## Legal risks
1. Data protection risks*
2. Risks from changes in jurisdiction
3. Licensing risks
4. Subpoena & e-discovery
## Cloud Computing

### Cloud Computing Risk Areas

**General risks related to Cloud Computing**

1. Network breaks
2. Network mgt
3. Modifying network traffic
4. Privilege escalation
5. Social engineering attacks
6. Loss or compromise of operational logs
7. Loss or compromise of security logs
8. Customization
9. Integration with other applications
10. Backups stolen/lost
11. Unauthorized access to premises
12. Theft of IT equipment
13. Natural disasters

### Cloud Computing Top Risk Areas

**Long term viability of provider.**

**Failure to perform agreed-upon service levels**

- impacting confidentiality, integrity and availability

**Confusion where information actually resides.**

**Privileged user access to sensitive information.**

**Data isolation/segregation**

**Compliance to regulations & laws**

**Information recovery in the event of disaster.**

*ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2010*
Cloud Computing

AGENDA

- Introduction
- Security
- Governance
- Risks
- Compliance
- Recommendations
- References

Cloud Computing Compliance “Tools”

- ISO 27000  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
- BS 25999  Business Continuity
Cloud Computing

AGENDA

• Introduction
• Security
• Governance
• Risks
• Compliance
• Recommendations
• References

10 recommendations for proper Cloud Computing

1. Executive management vision – decision – support
2. Clear roles & responsibilities (RACI)
3. Link with the business plan (business case)
4. Validated & well articulated business risks (and response)
5. Proper identity & access management controls
6. Methods for buy/build analysis with cost/benefit end-to-end model approved by all relevant stakeholders
7. Continuous communication
8. Inspect what you expect
9. Find a good lawyer who understands IT
10. Never outsource what you do/can not manage anyway!
Cloud Computing

AGENDA

• Introduction
• Security
• Governance
• Risks
• Compliance
• Recommendations
• References

References: Relevant Cloud Computing Books

• Cloud Computing: technologies & strategies of the ubiquitous data center, Curtis Franklin & Brian Chee, 288 pages, February 2010
• Above the Clouds: managing risk in the world of cloud computing, Kevin Mcdonald, February 2010
• Cloud Computing for dummies, Judith Hurwitz-Robin Bloor-Marcia Kaufman, 310 pages, November 2009

Marc Vael
Across
ISACA Belgium
May 2010
Cloud Computing

References: Relevant Cloud Computing websites

- www.cloudsecurityalliance.org/
- csrc.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/cloudcomputingresources

Contact information

Mr. Marc Vael
Partner

Across Technology
Innovatie- en Incubatiecentrum
Technologiepark 3
9052 Gent

Tel: 09 243 60 00
Fax: 09 243 60 06
Mail: marc.vael@a-cross.com