The Perfect Storm: Threats and Risks in the Cloud

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
Security Strategist & Evangelist
Quest Software

ISACA’s Guidance & Practices Committee Member
A TRUE STORY
OF MEN AGAINST THE SEA

THE
PERFECT
STORM

“A white-knuckle adventure.”
—Newsweek

SEBASTIAN
JUNGER
What is Cloud?

The biggest evolution in technology that can have an impact similar to the birth of the Internet

Number 1 on the list of ‘10 strategic technologies’ of all the analysts

‘Unless you’ve been under a rock recently, you’ve probably heard Cloud Computing as the next revolution in IT’ - CFO Magazine
What is Cloud?

A pay-as-you-go model for using applications, development platforms and/or IT infrastructure
Client Assumes All Data and Application Security Risks

IaaS
Infrastructure as a Service
- APIs
- Core Connectivity and Delivery
- Abstraction
- Hardware
- Facilities

PaaS
Platform as a Service
- Integration and Middleware
- APIs
- Core Connectivity and Delivery
- Abstraction
- Hardware
- Facilities

SaaS
Software as a Service
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content

Data and Application Security Risks Per SLA

Source: Universal Model, © Cloud Security Alliance. Used with permission.
Corporate mandates

**Manage risk**
- Compliance
- Asset protection
- Continuity Management

**Manage operational and business risk**

**Manage cost**
- Optimize resources
- Automate processes

**Better CAPEX and OPEX management**

**Improve service**
- Service Availability
- Service Management

**Optimal value providing effective and efficient services**

**Align IT investments**
- IT Portfolio Management
- Value Management
- Process Management

**Align investments with corporate objectives**
Cloud Benefits

Optimized use of infrastructure
Cost savings
Dynamic scalability
Optimized software development lifecycle
Reduced deployment time
Cloud Challenges

Data location
Shared infrastructure
Transparency on policies and procedures
Ownership of data
Proprietary APIs and vendor lock-in
Information protection for forensic analysis
Identity and Access Management
Legal requirements
Data deletion on SaaS or PaaS
Reasons for not using Cloud

Source: ISACA – Global Status Report on the Governance of Enterprise IT (GEIT) - 2011
Cloud Adoption

- Security concerns: 79%
- Manageability: 12%
- Cost: 9%

Priorities

- Security: 59%
- Management: 27%
- Monitoring: 17%
- Availability: 7%

Sources: IBM survey 2010, Ponemon Institute, CA Technologies, ISACA, ENISA, CSA
TICKETS

CLOSED
NEXT WINDOW
PLEASE

NEXT WINDOW PLEASE
Business-driven
Cloud domains

Cloud Architecture

Governance and Enterprise Risk Management

Legal and Electronic Discovery

Compliance and Audit

Information Lifecycle Management

Portability and Interoperability

Security, Business Continuity and Disaster Recovery

Data Center Operations

Incident Response, Notification, Remediation

Application Security

Encryption and Key Management

Identity and Access Management

Virtualization
Cloud Management Frameworks
Business Model for Information Security
Key Cloud Security problems

From CSA Top Threats Research

Trust: Lack of Provider transparency. Impacts Governance, Risk & Compliance

Data: Leakage, Loss or Storage in unfriendly geography

Insecure Cloud software

Malicious use of Cloud services

Account/Service Hijacking

Malicious Insiders

Cloud-specific attacks
Enterprise Risk

- Strategic Risk
- Environmental Risk
- Market Risk
- Credit Risk
- Operational Risk
- Compliance Risk

IT-related Risk

- IT Benefit/Value Enablement Risk
- IT Programme and Project Delivery Risk
- IT Operations and Service Delivery Risk
What?
Who?
Where?
How?
When?
Why?
IT CONTROL OBJECTIVES for CLOUD COMPUTING: CONTROLS AND ASSURANCE IN THE CLOUD
Example of Control Objectives

Cloud Computing COBIT Control Objectives

<table>
<thead>
<tr>
<th>COBIT Domain: Plan and Organize (PO)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P01 Define a Strategic IT Plan</strong></td>
</tr>
<tr>
<td>IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resources requirements and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.</td>
</tr>
</tbody>
</table>

| **P01.1 IT Value Management** |
| Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable SLAs. Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits. |

| **P01.2 Business-IT Alignment** |
| Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment. |

<table>
<thead>
<tr>
<th>Cloud Deployment Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Priority</strong></td>
</tr>
<tr>
<td>Public: □ □ □ □</td>
</tr>
<tr>
<td>Private: ● ● ● ●</td>
</tr>
<tr>
<td>Hybrid: ▲ ▲ ▲ ▲</td>
</tr>
<tr>
<td><strong>Lower Priority</strong></td>
</tr>
<tr>
<td>□ □ □ □ □ □ □ □</td>
</tr>
</tbody>
</table>

2011-November
ISACA Valencia - V Congress
## Assurance in the Cloud

<table>
<thead>
<tr>
<th>2. GOVERNING THE CLOUD (CONT.)</th>
<th>COBIT Cross-reference</th>
<th>COSO Reference</th>
<th>Issue Cross-reference</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance Model</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control: The organization has mechanisms in place to identify all providers and brokers of cloud services with which it currently does business and all cloud deployments that exist across the enterprise. The organization ensures that customer, IT, information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the organization.</td>
<td>D5.1</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>2.1.1.1 Determine if the IT, information security and key business functions have defined integrated governance framework and monitoring processes.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2.1.1.2 Determine if the IT, information security functions and key business units are actively involved in the establishment of SLAs and contractual obligations.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2.1.1.3 Determine if the information security function has performed a gap analysis of the service provider’s information security capabilities against the organization’s information security policies and threat and vulnerabilities/IT risk emanating from the transition to cloud computing.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2.1.1.4 Determine if the cloud provider has identified control objectives for the provided services.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-level Risk Scenarios</td>
<td>Positive Example Scenarios</td>
<td>Negative Example Scenarios</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New (cloud) technologies</td>
<td>• New technologies for new initiatives or more efficient operations adopted and exploited</td>
<td>• Failure to adopt and exploit new technologies (i.e., functionality, optimization) on a timely basis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Competitive advantage</td>
<td>• New and important technology trends not identified</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Business innovation potential</td>
<td>• Inability to use the technology to realize desired outcomes (e.g., failure to make required business model or organizational changes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Cloud) technology selection</td>
<td>• Optimal technology selected for implementation</td>
<td>• Wrong technologies (i.e., cost, performance, features, compatibility) selected for implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ability to switch faster to newer technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud investment decision making</td>
<td>• Coordinated decision making over IT investments between business and IT</td>
<td>• Business managers or representatives not involved in important IT investment decision making (e.g., new applications, prioritization, technology opportunities)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reduced IT investment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability over cloud (IT)</td>
<td>• Business assumes appropriate accountability over IT and codetermines the strategy for the cloud, especially application portfolio</td>
<td>• Business not assuming accountability over those cloud areas that it should (e.g., functional requirements, development priorities, opportunity assessment through new technologies)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security is paramount
Training and education
Useful resources
10 questions to ask to the Cloud

- How is identity and access managed in the Cloud?
- Where will my data be geographically located?
- How securely is my data handled?
- How is access by privileged users controlled?
- How is data protected against privileged user abuse?
- What levels of isolation are supported?
- How is my data protected in virtual environments?
- How are the systems protected against Internet threats?
- How are activities monitored and logged?
- What kind of information security certification do you have?
THANK YOU

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
Security Strategist & Evangelist - Quest Software
ramses.gallego@quest.com
THANK YOU

GRACIAS

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
Security Strategist & Evangelist
Quest Software
ramses.gallego@quest.com