A Comparison of IT Governance & Control Frameworks in Cloud Computing

Jack D. Becker
ITDS Department, UNT
&
Elana Bailey
ITDS Department, UNT
MS in IS

AMCIS 2014 August, 2014 Savannah, GA
Presentation Overview

- Key Issues of IT Governance in the Cloud
- Current Control Frameworks and Models
- Cloud Control in IT Governance
- Cloud IT Governance - Control Dial
Governance

- Enterprise Governance
- Corporate Governance
- Security Governance
- IT Governance
- Cloud Governance
Key Issues

- Transparency of controls
- Which Control Framework?
- Compliance (legal, regulatory, and audit)
- Transborder information flow
- Privacy and security
- International regulation and policy
- Corporate cultural impacts
Current Popular Control Frameworks and Models

Comparison of Popular IT Standards & Control Frameworks

- ISACA CobiT for Cloud Computing (2011)
- Cloud Cube Model (Jerico Forum; 2012)
- COSA – ERM Framework (2012)
- ENISA (Europe/COSO Model; 2009)
- ISO 27000/9000 (2011)
ISACA IT Control Objectives
Information Systems Audit and Control Association

Control Objectives for Information and Related Technology

Source: Cloud Security Alliance, https://cloudsecurityalliance.org
Cloud Cube Model

Source: www.jerichoforum.org
How risks and controls are viewed
Align organization objectives
Identify opportunities or risks
Determine impact of risks
Mitigate risks
Assign control responsibility (organization or CSP)
Establish timely and accurate communication flows
Monitor effectiveness
ENISA Governance Framework
European Network and Information Security Agency

Based on COSO's Internal Control Integrated Framework

Source: http://sysonline.net/content.php?id=53
ISO 27001 - 27002
International Organization for Standardization

Source: http://www.simosindia.in/services/plan/?id=iso
<table>
<thead>
<tr>
<th>Operational Domains</th>
<th>Governance Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Security, Business Continuity and Disaster</td>
<td>Governance and Enterprise Risk Management</td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
</tr>
<tr>
<td>Data Center Operations</td>
<td>Legal and Electronic Discovery</td>
</tr>
<tr>
<td>Incident Response, Notifications and Remediation</td>
<td>Compliance and Audit</td>
</tr>
<tr>
<td>Application Security</td>
<td>Information Lifecycle Management</td>
</tr>
<tr>
<td>Encryption and Key Management</td>
<td>Portability and Interoperability</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
</tr>
</tbody>
</table>
PDCA Cycle
aka Deming or Shewhart Cycle

- **PLAN** – create the requisite objectives and processes
- **DO** – implement the processes
- **CHECK** – evaluate and monitor the defined processes
- **ACT** – modify the processes for improvement
# Summary of Frameworks and Models

<table>
<thead>
<tr>
<th>Cloud Governance Models and Frameworks</th>
<th>Policies and Processes Adaption</th>
<th>Control and Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO ERM</td>
<td>Risk assessment</td>
<td></td>
</tr>
<tr>
<td>ISACA</td>
<td>Business Process Handling</td>
<td>Audit and Assurance Program</td>
</tr>
<tr>
<td></td>
<td>IT-business alignment</td>
<td>Risk IT</td>
</tr>
<tr>
<td></td>
<td>CobiT</td>
<td>Val IT</td>
</tr>
<tr>
<td>ITIL</td>
<td>Best Practices</td>
<td>Cloud provider audit recommendations</td>
</tr>
<tr>
<td></td>
<td>Process management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security management adaptation</td>
<td></td>
</tr>
<tr>
<td>ISO 27000 series &amp; ISO 9000</td>
<td>Standards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assurance</td>
<td></td>
</tr>
<tr>
<td>ENISA</td>
<td>Recommendations and check list: questions to provide assurance</td>
<td></td>
</tr>
<tr>
<td>Cloud Cube Model</td>
<td>Collaboration Lifecycle</td>
<td>Audit and compliance from collaboration oriented architecture</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>CSA Security Guidance</td>
<td>Collaboration programs</td>
<td>CloudAudit</td>
</tr>
<tr>
<td></td>
<td>Redefine role and responsibilities</td>
<td></td>
</tr>
<tr>
<td>PDCA</td>
<td>Process Refinement</td>
<td>PDCA cycle for control functions</td>
</tr>
</tbody>
</table>
### Cloud Governance

**Governance is both a framework and a process**

<table>
<thead>
<tr>
<th>Governance framework</th>
<th>Governance process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate framework</td>
<td>Governance processes</td>
</tr>
<tr>
<td>IT framework</td>
<td>Standing governance</td>
</tr>
<tr>
<td>Corporate strategy</td>
<td>Project governance</td>
</tr>
<tr>
<td>Corporate values</td>
<td>Governance mechanisms</td>
</tr>
<tr>
<td>Business model</td>
<td>Structures</td>
</tr>
<tr>
<td>IT strategy</td>
<td>Roles</td>
</tr>
<tr>
<td>IT principles</td>
<td>Tools</td>
</tr>
<tr>
<td>Enterprise architecture</td>
<td></td>
</tr>
</tbody>
</table>

Figure 7: Practical Governance, (2010). Retrieved from Gartner database.
5 IT Governance Domains

Integrating Cloud IT Governance Models and Frameworks:
Extending IT Governance to the Cloud Issues to Consider

- Internal Threats
- Horizontal Audit Compliance
- Performance Metrics (SLAs)
- Security (SecaaS)
- Accountability & Responsibility
  - RACI Matrix
Accountability & Responsibility

ACCOUNTABILITY
- Preventive Controls
- Detective Controls
- Procedural Measures
- Technical Measures

RESPONSIBILITY
- Customer vs. Provider
- Compliance
- Data Management
- Forensics & Recovery

RACI Matrix:
Responsible; Accountable; Counsel; Informed
Deconstructing the Cloud: Assess Each Item to be Moved!

1. What is Moving to the Cloud?
   Application Domain or Business Process
2. How will it be delivered?
   SaaS, IaaS, PaaS, BPMaaS
3. How will it be deployed?
   Public, Private, Community/Managed, or hybrid

Note: There are 16 possible Delivery and Deployment possibilities
Deconstructing the Cloud:
Next Step (Jericho Cube Model):

4. Where will the Data be Located? Internal or External?
5. Who Owns the technology, services and interfaces? Proprietary or Open?
6. Are there expectations of collaboration and data sharing? Perimeterized or De-Perimeterized?
7. Who is managing the delivery? Insourced or Outsourced?
IT Risk Management -- Westerman’s Hierarchy

- Agility – Strategic Risk
- Accuracy – Data Integrity Risk
- Access Risk Management
- Availability – Business Continuity
Cloud Governance Dial
1. What is Moving to the Cloud?
2. IT Governance Domain Objectives & Deliverables
3. Delivery Method?
4. Deployment Approach?
5. Cloud Formation Approach?
6. Enterprise Risk Management Controls?
7. IT Cloud Governance
8. Evaluation, Improvements, and Adaptation
Visualizing an Example of Using the Governance Dial
Conclusion

- Achieve IT-business alignment
- Add value