IT Governance in Cloud Computing

Presentation Topics

- Key Issues of IT Governance in the Cloud
- Frameworks and Models
- Cloud Control in IT Governance
- Critical Success Factors
Governance

Key Issues

- Transparency of controls
- Compliance (legal, regulatory, and audit)
- Transborder information flow
- Privacy and security
- Certification
- International regulation and policy
- Corporate cultural impact
Frameworks and Models


COSO ERM Framework
Committee of Sponsoring Organizations of the Treadway Commission

Source: (Crowe Horwath LLP, Chan, Leung, & Pili, 2012)
ISACA IT Control Objectives
Information Systems Audit and Control Association

[Image: ISACA IT Control Objectives diagram]

Control Objectives for Information and Related Technology

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

ITIL
Information Technology Infrastructure Library

[Image: ITIL diagram]

Source: http://sysonline.net/content.php?id=33
ISO 27001 - 27002
International Organization for Standardization

ENISA Governance Framework
European Network and Information Security Agency

Based on COSO's Internal Control Integrated Framework

## Cloud Cube Model

Source: www.jerichoforum.org

## CSA Cloud Security Guidance
Cloud Security Alliance

<table>
<thead>
<tr>
<th>Operational Domains</th>
<th>Governance Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Security, Business Continuity and Disaster Recovery</td>
<td>Governance and Enterprise Risk Management</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>CO90 ERM</td>
<td>Risk assessment</td>
<td>Audit and Assurance Program</td>
</tr>
<tr>
<td>ISACA</td>
<td>Business Process Handling</td>
<td>Risk IT</td>
</tr>
<tr>
<td></td>
<td>IT-business alignment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CobIT</td>
<td></td>
</tr>
<tr>
<td>ITIL</td>
<td>Best Practices</td>
<td>Cloud provider audit recommendations</td>
</tr>
<tr>
<td>ISO 9000 series &amp; ISO 27000</td>
<td>Process management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security management adaptation</td>
<td></td>
</tr>
<tr>
<td>ENISA</td>
<td>Standards</td>
<td></td>
</tr>
<tr>
<td>Cloud Cube Model</td>
<td>Recommendations and check list</td>
<td>Audit and compliance from collaboration oriented architecture</td>
</tr>
<tr>
<td></td>
<td>questions to provide assurance</td>
<td></td>
</tr>
<tr>
<td>C&amp;A Security Guidance</td>
<td>Collaboration program</td>
<td>CloudAudit</td>
</tr>
<tr>
<td></td>
<td>Collaboration lifecycle</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>PDCA</td>
<td>Process Refinedness</td>
<td>PDCA cycle for control functions</td>
</tr>
</tbody>
</table>
Cloud Control

Governance is both a framework and a process

Accountability & Responsibility

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

RESPONSIBILITY
- Customer vs. Provider
- Compliance
- Data Management
- Forensics & Recovery
Extending IT Governance to the Cloud

- Internal Threats
- Horizontal Audit Compliance
- Performance Metrics
- Security

Critical Success Factors

- Risk Management
- Audit Controls
- Integration Management
- Records Management & Data Mapping
- Controls: authentication, access, encryption
Conclusion

- Achieve IT-business alignment
- Add value