Security, Compliance & Risk Management for Cloud Relationships

Adnan Dakhwe, MS, CISA, CRISC, CRMA

Safeway Inc.

In-Depth Seminars – D32
Introductions & Poll

- Organization is **leveraging** the Cloud?
- Organization is **considering** leveraging the Cloud?
- Have **done** review/assessment of Cloud Service Providers?
- Will be **doing** a review/assessment of Cloud Service Providers?

2014 Fall Conference - "Think Big"
October 13-15, 2014
# Agenda

- Cloud 101/Overview
- Current Trends in Cloud Computing
- Benefits of Cloud Computing
- Risks and Challenges Companies Need to Consider
- Corporate Cloud Strategy and Governance – COSO ERM for Cloud Computing
- Key Considerations for Security, Compliance and Risk Management for Cloud Relationships
- Resources/Best Practices from ISACA and CSA
Cloud 101/Overview
What is Cloud Computing?

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.\(^1\)

---

1 – SP 800-145 - The NIST Definition of Cloud Computing
NIST Visual Model of Cloud Computing

Cloud Computing Service and Deployment Models

Source – ISACA – IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud
Jericho Forum – Cloud Cube Model

Levels of Control by Cloud Service Model

Source – COSO – ERM for Cloud Computing
Cloud Deployment Models

<table>
<thead>
<tr>
<th>Public</th>
<th>Infrastructure Managed By(^1)</th>
<th>Infrastructure Owned By(^2)</th>
<th>Infrastructure Located(^3)</th>
<th>Accessible and Consumed By(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
<td>Off-Premise</td>
<td>Untrusted</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Private/Community</th>
<th>Organization</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Or</td>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Hybrid            | Both Organization & Third Party Provider | Both Organization & Third Party Provider | Both On-Premise & Off-Premise | Trusted & Untrusted |

\(^1\) Management includes: governance, operations, security, compliance, etc...

\(^2\) Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

\(^3\) Infrastructure Location is both physical and relative to an Organization’s management umbrella and speaks to ownership versus control

\(^4\) Trusted consumers of service are those who are considered part of an organization’s legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Current Trends in Cloud Computing
Trends in Cloud Computing

Corporate spending on cloud infrastructure and services is forecast to triple from 2011 to 2017 to a projected $235.1 billion.¹

¹ – IHS Technology Study

Cloud IT Spending Soars
Global spending forecast by enterprises on cloud architecture

Source: IHS

1 – IHS Technology Study
Trends in Cloud Computing

The global cloud computing market is expected to grow at a 30% compound annual growth rate (CAGR) reaching $270 billion in 2020.¹

Gartner Magic Quadrant for SaaS - CRM Customer Engagement Center
Gartner Magic Quadrant for Enterprise Application PaaS

As of January 2014
Gartner Magic Quadrant for IaaS

As of May 2014

Leaders
- Amazon Web Services
- Microsoft

Visionaries
- CenturyLink
- CSC
- IBM (SoftLayer)
- Verizon Terremark
- Google

Niche Players
- Dimension Data
- Joyent
- Fujitsu
- GoGrid
- HP

Challengers
- Virtustream
- Rackspace

Ability to Execute

Completeness of Vision
New Service Offerings

- Disaster Recovery as a Service - DRaaS
- Security as a Service – SecaaS
- Identity as a Service – IDaaS
- Data Analytics as a Service – DAaaS
- Data Storage as a Service - DSaaS
- Information as a Service (InfoaaS)
- Integration Platform as a Service (IPaaS)
- Forensics as a Service (FRaaS)

Source – ISACA – Controls and Assurance in the Cloud Using COBIT 5
Benefits of Cloud Computing
Benefits of Cloud for User Organizations (Customers)

• Cost savings/reduction/management – lower entry costs, pay as you go, CAPEX to OPEX, reduced hardware infrastructure costs, reduced IT staffing and administration costs, etc.
• Scalability
• Flexibility/agility and speed of deployment
• Environmental benefits – power reduction for the user company, enhancement of user company’s “green” credentials
• Optimized server utilization
• Access to capabilities/skills which are not in-house
• Faster cycle of innovation
Risks and Challenges Companies Need to Consider
Risks and Challenges

• Vendor Management - inadequate contracts (right to audit clause, etc.), service provider viability, financial stability, etc.
• Regulatory Compliance – PCI, HIPAA, SOX, GLBA, etc.
• Data Security and Privacy – data location, co-mingled data/data segregation, loss of control over data, consolidation of multiple organizations presents a more attractive target for attacks, physical security, etc.
• Reliability, Availability and Performance – SLAs, etc.
• Termination of Services - vendor lock-in, portability and interoperability, etc.
• Business Continuity, Disaster Recovery and Resilience
• Shadow IT
• Access Control and Identity Management
• Governance
• Integration with existing systems
• Record protection/support for forensic audits
• Incident Management
Recent Cloud Outages

- Microsoft Cloud Service Azure Experienced Global Outage – August 13, 2014 – Lasted around 5 hours
- Microsoft Exchange – June 24, 2014 - Almost 9 hours – networking infrastructure issue
- Microsoft Lync – June 23, 2014 – several hours - network routing infrastructure issues
- iCloud – June 12, 2014 – few hours
- Feedly – June 11 – 13, 2014 – on and off for 3 days – DDoS attack
- Evernote – June 10, 2014 – 10+ hours – DDoS attack
- Adobe Creative Cloud service – May 16, 2014 – About 28 hours - database maintenance activity caused the outage
- Samsung's Smart TV platform global outage – April 20, 2014 – 4.5 hours – fire at one of the facilities in South Korea, was sparked by a failure with a power supply.
- Basecamp goes offline – March 24, 2014 – Around 2 hours – due to DDoS attack
- Google Apps – March 17, 2014 – About 3.5 hours – maintenance gone wrong
- Dropbox – March 2, 2014 – Just under an hour
- Gmail, Google Calendar, Google Docs, and Google+ go offline – January 24, 2014 – About an hour – software bug
- Dropbox – January 10, 2014 – About 2 days - a scripting glitch caused OS upgrades to be applied on actively running machines during routine maintenance.

Corporate Cloud Strategy and Governance – COSO ERM for Cloud Computing
Corporate Cloud Strategy and Governance: COSO ERM Framework for Cloud Computing

Corporate Cloud Strategy and Governance

Some of the governance and monitoring aspects for cloud relationships can be automated using tools; e.g., from Netskope or Skyhigh Networks.
Key Considerations for Security, Compliance and Risk Management for Cloud Relationships
Key Considerations for Security, Compliance and Risk Management

- Strategy - Evaluate if cloud is right for you as an option for IT sourcing?
- Give a deep thought before putting mission critical data in the cloud
- Assess Cloud Service Providers (CSP) – SOC 1/2/3, ISAE 3402, ISO 2700x, STAR Registry, OCF, CAIQ, CCM, etc.
- Contract - Ensure adequate terms, conditions and SLAs
- Support for eDiscovery and forensic audits
- Encrypt any sensitive data or use tokenization
- Ensure compliance requirements are met
- Ensure adequate identity and access management for users including CSP staff
- Secure disposition of data from servers including backups
- Define termination/exit and portability items upfront
- Governance and monitoring
- Business continuity and disaster recovery
- Backups
- Information security
- Physical security
Information Security Considerations

- Policies and procedures
- IPS/IDS, penetration testing and vulnerability management
- Adequate authentication controls
- DLP, antivirus, anti-malware, log management and file integrity management
- Web application security – web application firewall (WAF), encryption (data at rest and in motion) or tokenization, key management, etc.
- Incident response plan
- Configuration, change and patch management
- Security Information Event Management (SIEM)
- Virtualization security and controls
- Make sure your (customer organization) internal security is up to date. Don’t let your corporate network become the weakest link in the chain.
Key Points to Consider for Contracts

- Right to audit clause
- Third party assurance of controls – SOC 1/2/3, ISAE 3402, ISO 27001, etc.
- Financial performance monitoring (needs to be negotiated in the contract for private service providers)
- Governance and monitoring
- Regulatory compliance
- Dispute resolution and termination
- Information Security and physical security requirements – IPS/IDS, WAF, penetration testing, vulnerability management, SIEM, etc.
- Service level agreements and reporting procedures
- Recourse and remediation of unsatisfactory performance
- Data breach liability
Key Points to Consider for Contracts

- Incident management
- Confidentiality/Intellectual Property
- Disaster recovery and business continuity
- Sub-contracting – i.e., CSP is leveraging other CSPs
- eDiscovery and forensics
- Handling of sensitive data – encryption
- Disposition of data
- Term of contract
- Billing provisions
- Non-disclosure
Resources/Best Practices from ISACA and CSA
ISACA – Security Considerations for Cloud Computing

ISACA Cloud Resources – Security, Compliance and Risk Management

Source - http://www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx
ISACA Cloud Resources – Security, Compliance and Risk Management

Source - http://www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx
CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

14 domains:
• Cloud Computing Architectural Framework
• Governance and Enterprise Risk Management
• Legal Issues: Contracts and Electronic Discovery
• Compliance and Audit Management
• Information Management and Data Security
• Interoperability and Portability
• Traditional Security, Business Continuity and Disaster Recovery
• Data Center Operations
• Incident Response
• Application Security
• Encryption and Key Management
• Identity, Entitlement and Access Management
• Virtualization
• Security as a Service

Source – https://cloudsecurityalliance.org/research/security-guidance/#_overview
CSA Cloud Controls Matrix (CCM)

• Control framework that gives detailed understanding of security concepts and principles
• Strengthens information security control environments by delineating control guidance by service provider and consumer, and by differentiating according to cloud model type and environment
• Maps to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, COBIT, PCI, NIST, NERC CIP, ENISA, COPPA, HIPAA/HITECH, AICPA 2014 Trust Services Criteria, etc.
• 133 controls

Source – https://cloudsecurityalliance.org/research/ccm/
CSA Cloud Controls Matrix (CCM) v3.0.1

AIS  Application & Interface Security
AAC  Audit Assurance & Compliance
BCR  Business Continuity Mgmt & Op Resilience
CCC  Change Control & Configuration Management
DSI  Data Security & Information Lifecycle Mgmt
DSC  Datacenter Security
EKM  Encryption & Key Management
GRM  Governance & Risk Management

HRS  Human Resources Security
IAM  Identity & Access Management
IVS  Infrastructure & Virtualization
IPY  Interoperability & Portability
MOS  Mobile Security
SEF  Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA  Supply Chain Mgmt, Transparency & Accountability
TVM  Threat & Vulnerability Management

Source – https://cloudsecurityalliance.org/research/ccm/
CSA Cloud Controls Matrix (CCM) v3.0.1

<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM v3.0 Control ID</th>
<th>Updated Control Specification</th>
<th>COBIT 5.0</th>
<th>COPPA</th>
<th>CSA Enterprise Architecture (formerly Trusted Cloud Initiative)</th>
<th>CSA Guidance v3.0</th>
<th>ENISA IAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface Security - Application Security</td>
<td>AIS-01</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., DVASAP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.</td>
<td>AP009.03</td>
<td>AP013.01</td>
<td>Application Services &gt; Development Process &gt; Software Quality Assurance</td>
<td>3.2.9 and 3.2.10</td>
<td>shared</td>
</tr>
<tr>
<td>Application &amp; Interface Security - Customer Access Requirements</td>
<td>AIS-02</td>
<td>Prior to granting customers access to data, assets, and information systems, identify security, contractual, and regulatory requirements for customer access shall be addressed.</td>
<td>AP009.01</td>
<td>AP009.02</td>
<td>BOSS &gt; Legal Services &gt; Contracts</td>
<td>3.2.3, 3.2.8 and 3.2.10</td>
<td>shared</td>
</tr>
<tr>
<td>Application &amp; Interface Security - Data Integrity</td>
<td>AIS-03</td>
<td>Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systemic processing errors, corruption of data, or misuse.</td>
<td>CSS06.02</td>
<td>CSS06.04</td>
<td>Application Services &gt; Programming Interfaces &gt; Input Validation</td>
<td>3.2.9 and 3.2.10</td>
<td>shared</td>
</tr>
<tr>
<td>Application &amp; Interface Security - Data Security &amp; Integrity</td>
<td>AIS-04</td>
<td>Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.</td>
<td>AP009.01</td>
<td>AP009.02</td>
<td>BOSS &gt; Data Governance &gt; Rules for Information Leakage Prevention</td>
<td>3.2.9 and 3.2.10</td>
<td>shared</td>
</tr>
<tr>
<td>Audit Assurance &amp; Compliance - Audit Planning</td>
<td>AAC-01</td>
<td>Audit plans shall be developed and maintained to address business process discrepancies. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audit.</td>
<td>AP012.04</td>
<td>AP012.05</td>
<td>BOSS &gt; Compliance &gt; Audit Planning</td>
<td>Title 16 Part 312</td>
<td>shared</td>
</tr>
</tbody>
</table>

Source – https://cloudsecurityalliance.org/research/ccm/
### CSA Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1

<table>
<thead>
<tr>
<th>Control Group</th>
<th>CGID</th>
<th>CID</th>
<th>Control Specification</th>
<th>Consensus Assessment Questions</th>
<th>AICPA TSC 2009</th>
<th>AICPA Trust Service Criteria (SOC 2SM Report)</th>
<th>AICPA TSC 2014</th>
<th>BITS SHA Assessment V5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface</td>
<td>AIS</td>
<td>-01.1</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.</td>
<td>Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Application Security</td>
<td></td>
<td></td>
<td></td>
<td>$3.10.0 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS</td>
<td>-01.2</td>
<td></td>
<td>Do you use an automated source code analysis tool to detect security defects in code prior to production?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS</td>
<td>-01.3</td>
<td></td>
<td>Do you use manual source code analysis to detect security defects in code prior to production?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS</td>
<td>-01.4</td>
<td></td>
<td>Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AIS</td>
<td>-01.5</td>
<td></td>
<td>(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source – [https://cloudsecurityalliance.org/research/cai/](https://cloudsecurityalliance.org/research/cai/)
CSA Security, Trust and Assurance Registry (STAR)

• **LEVEL ONE: CSA STAR Self-Assessment:** Cloud providers either submit a completed CAIQ, or to submit a report documenting compliance with CCM. Free offering.

• **LEVEL TWO: CSA STAR Attestation:** Collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM.

• **LEVEL TWO: CSA STAR Certification:** A rigorous third party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2005 management system standard together with the CSA CCM.

• **LEVEL THREE: CSA STAR Continuous Monitoring:** Currently under development and scheduled for 2015 release, CSA STAR Continuous Monitoring enables automation of the current security practices of cloud providers. Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts.

Source – [https://cloudsecurityalliance.org/star/](https://cloudsecurityalliance.org/star/)
CSA Security, Trust and Assurance Registry (STAR)

Source – https://cloudsecurityalliance.org/star/
Questions?
Contact Information

Adnan Dakhwe, MS, CISA, CRISC, CRMA
adnan.dakhwe@safeway.com
adnandakhwe@gmail.com
https://www.linkedin.com/in/adnandakhwe
Thank you!