Cloud Security Panel: Real World GRC Experiences

ISACA Atlanta’s 2013 Annual Geek Week
Agenda

• Introductions
• Recap: Overview of Cloud Computing and Why Auditors Should Care
• Reference Materials
• Panel/Questions
Introductions

• Grady Boggs, CISSP
  Technical Specialist, Security & Identity
  Microsoft Corporation

• Reid Eastburn, CISA, CRISC, CISM, HISP (Moderator)
  Vice President, Information Assurance and Security
  The Experts

• Stoddard Manikin, CISM, CISSP
  Director, Information Systems Security
  Children’s Healthcare of Atlanta

• Melanie Morris, CISM, CISSP, ISSAP, HISP, CISA
  Senior Manager, Risk & Information Security
  Cox Enterprises
Overview of Cloud Computing

- The use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)
- Extension of client-server model
- Cloud computing, big data, consumerization of IT (BYOD), and virtualization
  - Cloud computing adoption is one of the biggest IT trends.
Common Service Models of Cloud Computing

- IaaS (Infrastructure as a Service)
  - Measured service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Self-service

- PaaS (Platform as a Service)
  - SaaS (Software as a Service)

Source: NIST
Microsoft’s Cloud Environment

- Software as a Service (SaaS)
  - Consumer and Small Business Services
  - Enterprise Services
  - Third-party Hosted Services
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Global Foundation Services

- Microsoft Dynamics CRM Online
- Outlook
- Office 365
- Windows Azure

Data Centers, Operations, Global Network, Security
Why Auditors Should Care

• Risk typically stays “insourced”
• Organizations, and individuals, are outsourcing critical applications and data
• 24x7 pervasive availability also means your data is accessible to malicious users all day every day
• Multi-tenant architectures can result in unintended consequences, i.e., data mixing
• Cloud service providers may not share same goals (profitability vs. implementing controls)
• Providers don’t always follow industry standard security frameworks (ISO, NIST, FISMA, etc.)
Survey Data

• 51% of respondents, believe stormy weather can interfere with cloud computing.

• 54% of respondents claim to never use cloud computing.

• 97% are actually using cloud services today via online shopping, banking, social networking and file sharing.

Source: 1,000 surveyed by Wakefield research.
Adoption Risk and Rewards

**BENEFITS**
- scalability
- increased agility
- flexibility
- Reduced costs

**CONCERNS**
- privacy
- security
- reliability

Children’s Healthcare of Atlanta
Provider is your Partner
Reference Materials

• Cloud Security Alliance (CSA) – GRC Stack

• CSA – Security Guidance for Critical Areas of Focus in Cloud Computing

• CSA Security, Trust, and Assurance Registry
  – https://cloudsecurityalliance.org/star

• Microsoft Global Foundation Services
  – http://www.globalfoundationservices.com/

• Microsoft Cloud Security Readiness Tool
  – http://www.microsoft.com/trustedcloud
Panel

- Grady
- Reid
- Stoddard
- Melanie
Appendix
Common Deployment Models of Cloud Computing

• Public cloud
• Private cloud
• Hybrid cloud
• Community cloud
Security Maturity and Cloud Providers

• Trust us, we use a firewall

• We’ll be happy to fill out your questionnaire

• Download a copy of our 3rd party assessment

GRC must be built-in from the foundation, not bolted on as an afterthought
GRC and Cloud Computing

- Standards
- Encryption & Key Management
- Business Continuity / Disaster Recovery / Exit Strategy
- Transparency & Audit
- Identity and Access Management

Governance, Risk, & Compliance (GRC)

Information Risk Management Transition Planning

Copyright 2011 Cloud Security Alliance, Inc. All rights reserved
The GRC Stack Framework

Cloud Architecture
- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability
- Transparency

Operating in the Cloud
- Security, Bus. Cont., and Disaster Recovery
- Data Center Operations
- Incident Response, Notification, Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

Copyright 2011 Cloud Security Alliance, Inc. All rights reserved
GRC Examples in Cloud Computing

- Governance
  - Jurisdiction for contractual enforcement
  - Data governance
  - Transparency

- Compliance
  - ASP should follow a methodology (plan, do, check, act)
  - At end of the day, compliance can't be fully outsourced
  - Cloud provider's capabilities and controls must be integrated into your overall compliance program

- Risk
  - Employ a viable risk assessment and management process
  - Adopt a standards-based control framework
  - Consider insurance for losses
An Approach to Evaluate Cloud Providers

• Leverage the Cloud Security Alliance (CSA) GRC Stack
  – Cloud Controls Matrix
  – Consensus Assessments Initiative
  – Cloud Audit
  – CloudTrust Protocol

• Designed to support cloud consumers and cloud providers

• Prepared to capture value from the cloud as well as support compliance and control within the cloud

• Also review the Security, Trust, and Assurance Registry (CSA STAR)
  – Public registry of cloud provider self assessments
## Leveraging the CSA GRC Pack

<table>
<thead>
<tr>
<th>Delivering</th>
<th>Stack Pack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous monitoring ... with a purpose</td>
<td>CTP™</td>
<td>• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers</td>
</tr>
<tr>
<td>Claims, offers, and the basis for auditing service delivery</td>
<td>CloudAudit™</td>
<td>• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments</td>
</tr>
<tr>
<td>Pre-audit checklists and questionnaires to inventory controls</td>
<td>CAI™</td>
<td>• Industry-accepted ways to document what security controls exist</td>
</tr>
<tr>
<td>The recommended foundations for controls</td>
<td>CCM™</td>
<td>• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider</td>
</tr>
</tbody>
</table>
Example: Cloud Controls Matrix (CCM)

- First ever baseline control framework specifically designed for managing risk in the cloud

Copyright 2011 Cloud Security Alliance, Inc. All rights reserved
Closing Thoughts/Summary

• Concentrate on GRC as a foundational component of your organization’s cloud strategy
• Demand commitment to standards (CSA Cloud Controls Matrix) and transparency (CSA STAR)
• Encourage your cloud computing buyers and legal teams to require stipulations like “right to audit”
• Build familiarity with your vertical industry’s compliance needs
• Integrate your cloud provider's capabilities and controls into your overall compliance program
Cloud Security Panel
ISACA Geek Week 2013

Grady Boggs, cissp
Technical Specialist, Security & Identity
Microsoft Corporation

Stoddard Manikin
Directory of Security
Children’s Healthcare of Atlanta
Most Individuals confused by cloud computing

- **51%** of respondents, believe stormy weather can interfere with cloud computing.

- **54%** of respondents claim to never use cloud computing.

- **97%** are actually using cloud services today via online shopping, banking, social networking and file sharing.

1,000 surveyed by Wakefield research
What is cloud computing (NIST)
Risks and rewards of adoption

**BENEFITS**
- Scalability
- Increased agility
- Flexibility
- Reduced costs

**CONCERNS**
- Privacy
- Security
- Reliability
Provider is your partner

RESPONSIBILITY:

Data classification
Client and end point protection
Identity and access management
Application level controls
Host security
Network controls
Physical security

CLOUD CUSTOMER

IaaS
PaaS
SaaS

CLOUD PROVIDER
Microsoft’s Cloud Environment

- Consumer and Small Business Services
- Enterprise Services
- Third-party Hosted Services
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)

Global Foundation Services

- Security
- Global Network
- Operations
- Data Centers

Windows Azure

- Microsoft Dynamics CRM Online
- Outlook
- Office 365
Compliance Framework

INDUSTRY STANDARDS AND REGULATIONS
- ISO/IEC 27001:2005
- EU Model Clauses
- FISMA/NIST 800-53
- Sarbanes-Oxley
- PCI-DSS
- HIPAA, etc

CONTROLS FRAMEWORK
- Identify and integrate
  - Regulatory requirements
  - Customer requirements
  - Assess and remediate
  - Eliminate or mitigate gaps in control design

PREDICTABLE AUDIT SCHEDULE
- Test effectiveness and assess risk
- Attain certifications and attestations
- Improve and optimize
  - Examine root cause of non-compliance
  - Track until fully remediated

CERTIFICATION AND ATTESTATIONS
- ISO / IEC 27001:2005 certification
- SSAE 16/ISAE 3402 SOC 1
- AT 101 SOC 2 and 3
- PCI DSS certification
- FISMA certification and accreditation
- And more ...
Considerations for Choice in Cloud Services Provider

Consult guidance from organizations such as the Cloud Security Alliance

✓ Require that the provider has attained third-party certifications and audits, e.g. ISO/IEC 27001:2005

✓ Know the value of your data and processes and the security and compliance obligations you need to meet

✓ Consider the ability of vendors to accommodate changing security and compliance requirements

✓ Ensure a clear understanding of security and compliance roles and responsibilities for delivered services

✓ Ensure data and services can be brought back in house if necessary

✓ Require transparency in security policies and operations
Appendix
Cloud Security Alliance (CSA)

✓ Global not-for-profit organization
✓ Provider, and User Certification
✓ Accepted global authority for trust in the cloud
## Cloud Control Matrix (CCM)

<table>
<thead>
<tr>
<th>CCM control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DG-01</strong></td>
<td><strong>Data Governance - Ownership / Stewardship</strong>&lt;br&gt; All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.</td>
</tr>
<tr>
<td><strong>DG-02</strong></td>
<td><strong>Data Governance - Classification</strong>&lt;br&gt; Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.</td>
</tr>
</tbody>
</table>
Cloud Security Readiness Tool (CSRT)

Where are you now?

Where will you be?

Can cloud help?
**Equipment support contracts**

**Current State**
Equipment maintenance and replacement is handled inconsistently, and may not align with your operational needs.

**Recommendation**
A regular process for refreshing equipment should exist. This process should include regular reviews of support contract needs and a budget forecasting, and this effort should adhere to a capacity planning program.

**Advantage of moving to a Cloud service**

Keeping equipment up to date and in working order is essential for ensuring continuity of operations. Without current support contracts, obsolete or inoperative equipment can jeopardize the availability of important systems and information.

Cloud providers typically develop and maintain SCM processes that provide for continuity of operations and ensure ongoing security, compliance, and privacy protections. Equipment is refreshed regularly and all systems are kept current and operational. The process usually involves establishing alternate sites to be used in the event of failure of the primary service facility.
Control standards

- European Network and Information Security Agency (ENISA) - Information Assurance Framework (IAF)
- International Organization for Standardization (ISO 27001-2005)
- Payment Card Industry (PCI-DSS v2.0)
- Health Insurance Portability and Accountability Act (HIPAA-HiTech Act)
- National Institute of Standards and Technology (NIST SP800-53)
- American Electric Reliability Corporation (NERC CIP)
Commitment to Transparency Through STAR

Standard from the Cloud Security Alliance (CSA)
The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Microsoft’s Standard Responses on STAR
- Specific details about Office 365, Windows Azure and Dynamics CRM Security and Privacy is mapped to the CCM and the ISO certification.