
Auditing the Cloud
Paul Engle
CISA, CIA

About the Speaker

Paul Engle CISA, CIA

- Fifteen years performing internal audit, IT internal audit, and consulting projects
- Internal audit clients include ADP, Berwind Corporation, Center for Medicare and Medicaid Services (CMS), American Woodmark, Playtex Products, MothersWork, American Public Education, and Choice Hotels.
- Consulting clients include State of Arizona, AARP, HealthSouth, Allen and Shariff, Northwestern Human Services, and Konica-Minolta.

Learning Objectives

- ✓ Provide a framework and approach
- ✓ Discuss areas of highest risk
- ✓ Address your questions
- ✓ Provide an example or two
- ✓ Keep you awake
- ✓ Any others?

Let's make this more interesting!

Who Defined the Term "Cloud Computing"?

- Al Gore
- IBM
- Jeff Bezos
- Mell and Grance
- Bill Gates

Who Defined the Term "Cloud Computing"?

- Al Gore
- IBM
- Jeff Bezos
- Mell and Grance
- Bill Gates

Cloud Computing Definition

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources 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."

The NIST 800-145 Definition of Cloud Computing,

Peter Mell and **Timothy Grance**, September 2011

Cloud Computing Definition

- "Cloud computing is a model for enabling:
  - ubiquitous,
  - convenient,
  - on-demand network access
- to a shared pool of configurable computing resources 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."

5 Essential Characteristics

1. Broad-band access
2. On-demand self-service
3. Resource pooling
4. Rapid elasticity
5. Measured service

Metaphor

"IT services are delivered using a utility model"

3 Service Models

1. SaaS – Software as a Service
   - Salesforce, Google, Workday, Office 365, just about every new application…
2. PaaS – Platform as a Service
   - Microsoft Azure, many others…
3. IaaS – Infrastructure as a Service
   - Amazon Web Services (AWS), many others…

True or False?

AWS is the world's largest cloud provider.

Their SLA is 99.99% uptime.

And the answer is…

- Amazon Elastic Compute Cloud (EC2) = 99.95%
- Amazon Virtual Private Cloud (VPC) = 99.95%(?)
- Amazon Elastic Block Storage (EBS) = 99.95%
- **Amazon Simple Storage Service (S3) = 99.99%**
- Amazon Simple Database (Simple DB) = 99.95%(?)
- Amazon Relational DB Service (RDS) = 99.95%(?)
- Amazon Redshift = 99.95%(?)
- (many more)…

Source: Amazon Web Services

Amazon EC2 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2 or Amazon EBS, or any other Amazon EC2 or Amazon EBS performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2 or Amazon EBS; (iii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances or volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the AWS Agreement; or (vii) arising from our suspension and termination of your right to use Amazon EC2 or Amazon EBS in accordance with the AWS Agreement (collectively, the "Amazon EC2 SLA Exclusions"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Source: Amazon Web Services

4 Deployment Models

- Public Cloud
  - AWS, many others
- Private Cloud
  - Arizona State Data Center
- Hybrid Cloud
  - Public Cloud + Private Cloud
- Community Cloud

Why am I telling you this?

- Risk profiles may be ***very different*** for each Service and Deployment model
- Most audits are risk based, so the client's model matters

A LOT!

What Does CIA Stand For?

- Central Intelligence Agency
- Certified Internal Auditor
- Confidentiality, Integrity, Availability
- Culinary Institute of America
- All of the above

3 Risks

1. **Someone will compromise your data (Confidentiality)**
2. Someone or somethng will corrupt your data (Integrity)
3. Someone or something will prevent access to your data (Availability)

3 Risks

1. Someone will compromise your data (Confidentiality)
2. **Someone or something will corrupt your data (Integrity)**
3. Someone or something will prevent access to your data (Availability)

3 Risks

1. Someone will compromise your data (Confidentiality)
2. Someone or something will corrupt your data (Integrity)
3. **Someone or something will prevent access to your data (Availability)**

Confidentiality Risk

- Unauthorized or inappropriate disclosure of confidential information
- Examples
  - PII
  - Financial data
  - Government records and communications

Integrity Risk

- Unauthorized or inappropriate manipulation of information
- Examples:
  - Financial information
  - Student records
  - Attendance records

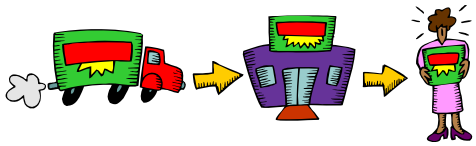
Availability Risk

- Data and / or services will become unavailable to users
- Examples:
  - Natural or man-made disasters
  - Distributed denial of service attacks
  - Cloud service provider fouls up
  - ISP goes down

Everyone's Nightmare

Government Reacts

Cloud Computing Risk Universe

- People 
- Process 
- Technology 

Cloud Risk Domains

1. Governance
2. Operations
3. Data Security and Encryption

Governance Domain

- Policies, standards and procedures
- How are providers selected and managed?
- Who is in charge of security?
- Who sets SLAs and monitors?
- How is risk management handled?
- How is compliance addressed?

Operations Domain

- How are incident response, notification and remediation addressed?
- How are services / performance monitored?
- Virtualization – what controls are in place?
- What happens when the client leaves the provider?

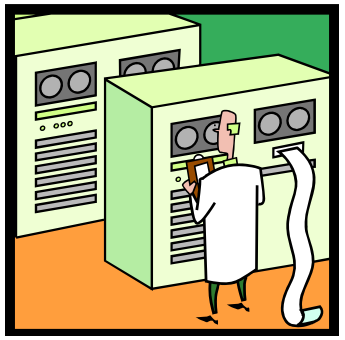
Data Security and Encryption

- Data in Transit – how strong is encryption? How is it managed?
- Data at Rest – how is this implemented and managed? Who's in charge?
- Key management!
- Access and Authentication – what's the process?
- DR and Business Continuity – Backups – who manages? How is it tested?

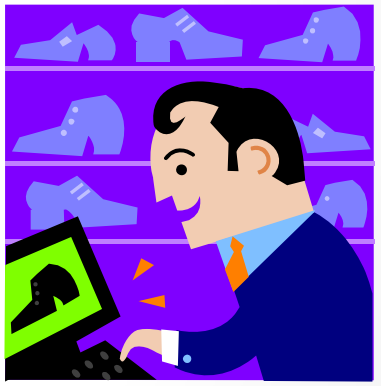
SaaS Risk

The Client or the Client's Client

The Client's Data



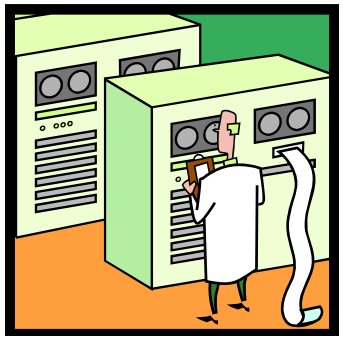
The Client's Provider



PaaS Risk

The Client or the Client's Client

The Client's Data



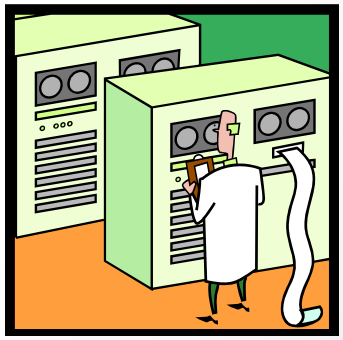
The Provider's Provider

IaaS Risk

The Client

The Client's Client

The Client's Data



Questions to ask…

- Who are the client's providers?
  - How do you know?
  - What controls do they offer?
  - Who decides / who manages?
- Who determines what data is stored?
- Where is the data stored?
- How is the data protected?
  - During data entry
  - During transport
  - During storage and retrieval
  - In the event of a disaster
  - In the event of a breach
- What happens in case of an "incident"?

Auditing 101

1. Scoping
2. Risk Assessment
3. Audit Planning
4. Gather evidence
5. Perform testing
6. Analyze results
7. Identify “issues”
8. Meet with client
9. Finalize results
10. Provide to client
11. Enter client response
12. Publish

Scoping

- Products, services, organization, risk appetite
- Supported business processes
- Service models
- Deployment models
- Locations
- Number, types of users
- Number, types of providers
- Types of data
- Number, types of applications
- Compliance requirements
- History
- Others?

Risk Assessment Data

- People
  - Who enters it
  - Who processes it and how
  - Who uses it
  - Who has access, and how is access controlled
- Process
  - How is it transported
  - How is it stored
- Technology
  - Reliability
  - Availability
  - Confidentiality
  - Compliance requirements

Audit Planning

- Identify and select an appropriate controls framework (e.g. CobiT, ISO, NIST, Cloud Security Alliance)
- Determine areas of highest risk
- Identify areas of change
- Identify past issues
- Decide how deep to dive

Gather Evidence

- Interview the key players
- Obtain:
  - Current policies, standards, and procedures
  - Equipment, service, provider, application, and data inventories
  - Network diagrams
  - Contracts including SLAs for key providers
  - Service logs
  - Results of penetration and vulnerability testing
  - DR and Business Continuity documents
  - Certificate documentation
  - SOC reports, ISO or PCI certifications, FedRAMP information

Perform Testing

- Identify the most important controls mitigating the areas of highest risk
- Examples:
  - Governance – who can add / terminate providers
  - Data classification
  - Change management
  - Certificate management / Encryption
  - Disaster recovery and testing
  - Privacy – who determines what PII to collect and where to store it

Analyze Results

- Compare identified controls to the appropriate framework:
  - What's there, what's missing, is it important
- Compare service logs to SLAs
  - Is the client receiving the appropriate level
- Compare service logs to policies and standards
  - Did the client do what they said they were going to do
- Analyze audit reports and certifications
  - Are there holes, and are the controls appropriate
- Review incidents and response

Identify Issues

- Focus on areas of highest risk
- Identify the issue and the associated risks
- Refer to the policy, standard, or control framework
- Provide realistic recommendations and examples, if appropriate

True or False

AWS provides adequate controls for data security

Shared Responsibility Environment

Moving IT infrastructure to AWS creates a **shared responsibility model** between the customer and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall. You should carefully consider the services you choose as your responsibilities vary depending on the services you use, the integration of those services into your IT environment, and applicable laws and regulations. It is possible for you to enhance security and/or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention, and encryption.

Source: Amazon Web Services: Overview of Security Processes June 2014

True or False

Providers offering SOC reports include adequate controls for data security

SOC Reports

Report	Standard	Intent / Usage	Report Contents
SOC-1 (Type 2)	SSAE No. 16 / AT 801 (AICPA)	• SOX • Financial Reporting	• Description of service organization's system. • CPA's opinion on fairness of description, suitability of design and operating effectiveness of controls. • Description of CPA's tests of controls and results
SOC-2 (Type 2)	AT 101 (AICPA)	• Security • Availability • Processing integrity • Confidentiality • Privacy (one or more)	
SOC-3	AT 101 (AICPA)		(Description of system and CPA's tests deleted)

Source: AICPA

True or False

FedRAMP is a new program designed solely for Federal Agencies

Source: http://cloud.cio.gov/fedramp

True or False

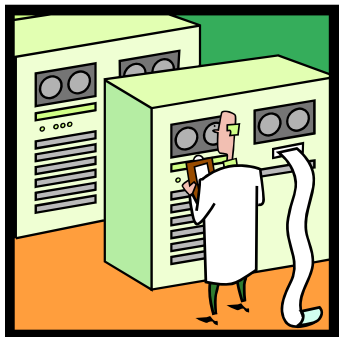
PCI – DSS 3.0 compliance insures adequate controls for data security


TARGET®

Example: SaaS Audit

The Client or the Client's Client

The Client's Data



The Client's Provider

Example: SaaS

Key risks – The Client or the Client's Client

1. Governance – who controls / manages the provider?
2. Access – who may enter / access the application?
3. Availability – who monitors performance vs. SLAs?

Example: SaaS

Key risks – Transport

- Type of encryption – who decides and who monitors? How?
- Certificates – how are they managed?
- Ports – which ports and why?
- Firewall – standard or next-generation?
- ISP – SLAs

Example: SaaS

Key risks – Data storage and processing

1. Encryption? How strong?
2. Certificates – how are they managed?
3. Provider controls
4. Authentication
5. Firewall
6. Anti-virus, penetration and vulnerability testing
7. Verification (SOC-2, FedRAMP, PCI)

Example: SaaS

Key risks – The Client's Provider

1. Change Management
2. Access / Authorization / Authentication
3. Firewall
4. Anti-virus, penetration and vulnerability testing
5. Verification (SOC-1, FedRAMP, PCI)

References

- Controls and Assurance in the Cloud: Using CobiT 5 (ISACA)
- Cloud Computing Management Audit / Assurance Program (ISACA)
- NIST SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
- FedRAMP Security Controls Baseline
- Cloud Security Alliance Cloud Controls Matrix
- Security Guidance for Critical Areas of Focus in Cloud Computing (CSA)
- Cloud Computing – Benefits, risks and recommendations for information security (ENISA)

Thank You!

Paul Engle CISA, CIA
paulfengle@outlook.com
443 629-1176