Auditing the Cloud

UHY LLP
Certified Public Accountants

David Barton
Principal, UHY LLP

UHY LLP Certified Public Accountants

Objectives

- Understand what Cloud Computing is
- Understand why Cloud is attractive
- Understand how it is the same as private computing
- Understand how it is different
- Present unique risks to Cloud Computing
- Suggest ways to control them

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

Cloud Adoption

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

Raise your hand if your company is…

- Using Cloud Computing Services
- Thinking about Cloud Computing Services
- Still trying to figure out what Cloud Computing is about

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

What is Cloud Computing?

"Cloud computing is a model for enabling 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."

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

What is Cloud Computing?

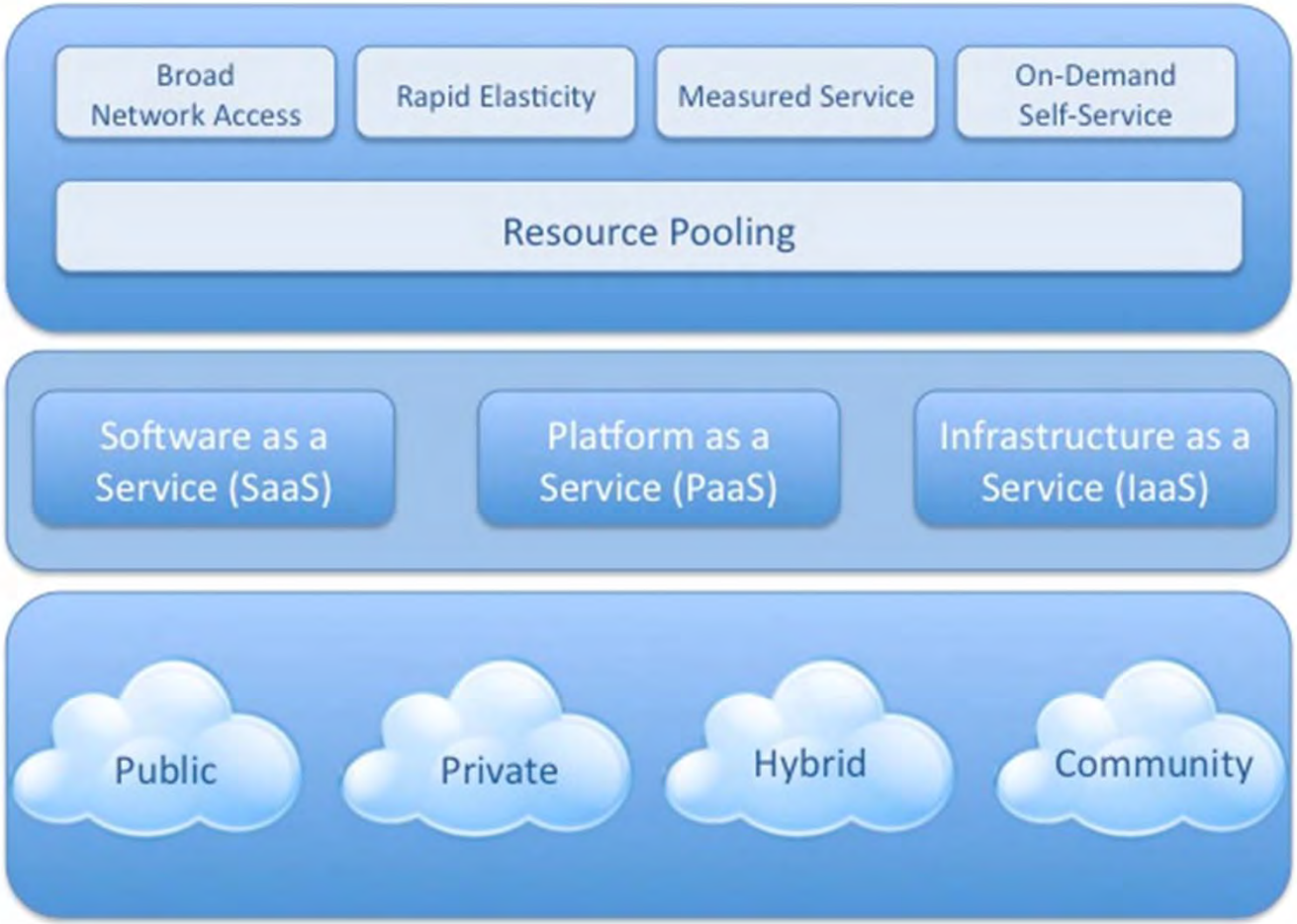
"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

Visual Model Of NIST Working Definition Of Cloud Computing

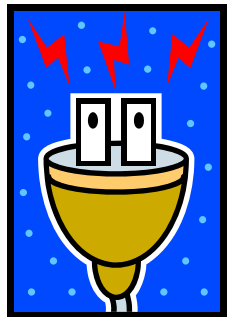
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



UHY LLP Certified Public Accountants

Why is Cloud Computing Attractive?

- Elasticity – rapid provisioning and scalability
- Efficiency – pay as you go
- On demand self service
- Resource pooling – shared expertise
- Ubiquitous availability – internet connectivity



THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Types of Cloud Services

Software as a Service (SaaS)

- Capability made available to tenant (or consumer) to use provider's applications running on cloud infrastructure, accessible via web browser, mobile apps, and system interfaces.
- *Examples*: Salesforce.com, Drop Box, Box.net, Google Docs, WebEx

Platform as a Service (PaaS)

- Capability made available to tenant to deploy tenant owned (created or acquired) applications using programming languages and tools supported by provider.
- *Examples*: Microsoft Azure, Amazon Web Services, Bungee Connect

Infrastructure as a Service (IaaS) / Datacenter as a Service (DaaS)

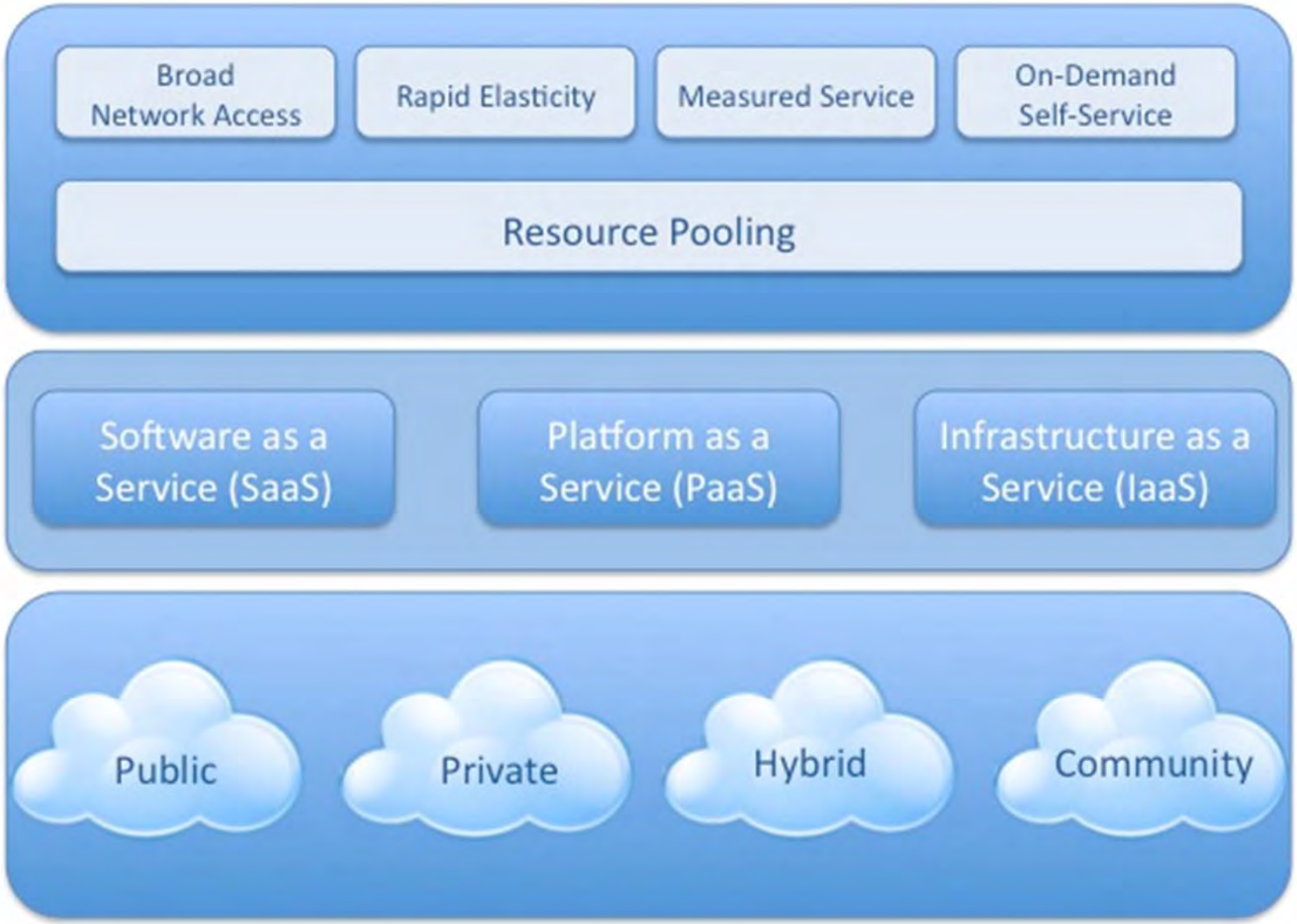
- Capability made available to tenant to provision processing, storage, networks or other fundamental computing resources to host and run tenant's applications.
- *Examples*: Rackspace, Terremark (Verizon), Savvis, AT&T

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



UHY LLP Certified Public Accountants

What Cloud is NOT

- Third party Data Center
- Co-location facility
- Managed Services

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Cloud vs. Private

- Risks are the same:

  Data Security
  - Confidentiality
  - Integrity
  - Availability
- Cannot outsource responsibility
- Risk can be:
  - Accepted (no action taken)
  - Transferred (bonding, insurance)
  - Mitigated (create controls)

UHY LLP Certified Public Accountants

Information Systems

Relevance to audit objectives consists of procedures and records established to:

- Initiate
- Authorize
- Record
- Process
- Report
- Maintain accountability
- Provide security

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Deficiency in Internal Control

- A ***deficiency in internal control*** exists when the *design* or *operation* of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

UHY LLP Certified Public Accountants

Risk Circumstances

- Changes in operating environment
- New personnel
- New / revamped information systems
- Rapid growth of entity
- New technology
- New business models, products, activities
- Corporate restructuring
- New or expanded foreign operations
- New accounting pronouncements

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Risk Circumstances

- Changes in operating environment
- New personnel
- New / revamped information systems
- Rapid growth of entity
- New technology
- New business models, products, activities
- Corporate restructuring
- New or expanded foreign operations
- New accounting pronouncements

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Security in the Cloud

"In the Cloud, step one is trusting, and that's not security — that's hope."

- Andrew Walls, Gartner Group

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Security Benefits of Cloud Computing

- Economies of Scale – security resources are cheaper when implemented on a larger scale
- Availability of expertise – more experts
- Standardized vulnerability management – virtual machines are generally pre-hardened and regularly updated with latest patches and security settings

UHY LLP Certified Public Accountants

Security in the Cloud

Key Difference = CONTROL

- Loss of Direct access - In the Cloud you are at least one step removed
- Multi-tenancy – not an issue in private computing, no shared devices or services
- Commingling – will your data be mixed in with other clients? How will it be segregated?
- Resource Pooling – how will resource conflicts be resolved? Who gets first response?

UHY LLP Certified Public Accountants

Security in the Cloud

- CP failure or acquisition – if your CP goes out of business or gets acquired by a competitor, where do you stand?
- Hypervisor compromise – If control of hypervisor is compromised, ALL virtual machines are at risk
- Ineffective data deletion – if you change providers does your data get destroyed? Unintentional destruction?
- Legal snafus – if Company A has their data subpoenaed and your data is also on the same device, what happens to your data?

UHY LLP Certified Public Accountants

Legal and Contract Issues

- Who? Responsible, Perform, Initiate
- What? Service (private, public, community), Options
- When? Alerts, reporting, audits
- Where? Data, facilities, call center, legal jurisdiction
- How? Measures, KPIs, escalation, penalties, alerts

UHY LLP Certified Public Accountants

Due Diligence

1. Is vendor viable?
2. Identity of data center operator and location - outside your home state? Outside of the US.?
3. Are subcontractors used?
4. How is client data segregated?
5. What technological/electronic measures are used to protect client data?
6. Is PCI or HIPAA compliance guaranteed? How?
7. Can operations deal with suspension of services?
8. How hard would it be to transition to a new vendor?
9. Confirm compliance with applicable bar (legal ethics)

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Data Security

Vital to select a vendor with adequate security:

1. Agreement should include minimum security and infrastructure practices;
2. Require that security practices be regularly updated;
3. Customer must have the right to perform regular audits to confirm compliance;
4. Third party verification and/or certification (e.g., ISO, SOC, PCI).

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Privacy Considerations

Information Privacy. If CP has access to sensitive data (SSN, account #, patient information, etc.), agreement should cover:

- Requirement to maintain all legal, technical and procedural compliance with consumer privacy laws;
- Social Security number laws; secure destruction and security procedures laws;
- Security breach notification laws (along with verification of incident response policy and reimbursement of costs arising from security breach); and
- Address user privacy and whether vendor has the right to retain and/or use data.

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SLAs and Performance

Identify concrete service level requirements:

- SLA definitions
- Availability/Uptime (e.g. 99.9%)
- Performance Standards per Transaction (load and response times)
- Scalability/Redundancy (address peak traffic capacity issues)
- Error correction time – Definition of “error”
- Problem Resolution and Notification (detail resolution of hosting issues, root cause analysis)
- Quality of service
- Root Cause Analysis
- Specify Penalties for Non-performance (liquidated damages/credits and termination rights)
- SLAs/KPIs unique to your business needs

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Transition from Current Provider

- Include a transition assistance provision requiring the vendor to assist customer with transition to a new vendor.
- Require the return or secure destruction of all data held by vendor.
- Have right to verify compliance.
- Transition period may last from 30 days to 6 months.

UHY LLP Certified Public Accountants

Recent Cloud "Events"

- Gmail outage Feb 2011 – 140,000 accounts lost
- Epsilon mail services breach – April 2011
  - Over 50 companies affected
  - Millions of email addresses (passwords?) compromised
- Amazon web services outage – April 2011

UHY LLP Certified Public Accountants

Suggested Actions

- Understand the risks
  - Educate yourself
  - Bring in experts
  - Determine impact on audit
- Mitigate the risks
  - Review Contract and SLAs
  - Third party audit (ISO, SOC 1, SOC 2, SOC 3)

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Suggested Actions

- Read the Service Auditor Report!!!
  - Does it cover all the pertinent risks?
  - Are all the control objectives covered?
  - Ask yourself “what is missing?”
  - Did the testing performed match your own criteria?
  - Were the sample sizes sufficient for the control?
  - Are there subservice organizations “carved out?”

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

Audits - Lack of Standards

PCI Security Standards Council

HIPAA
Health Insurance Portability & Accountability Act

ISAE 3402

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Summary of the Risks

- Cloud Computing lacks a broadly accepted standard for secure access and data handling
- Cloud Computing is not intended to be location specific– where is your data? If you don't know where your data is, you cannot hope to secure it.
- Cloud Computing is often pursued without adequate concern for security arrangements
- Cloud Computing presents new legal / contract issues
- Cloud Computing lacks a standard for third-party audit

UHY LLP
Certified Public Accountants

MISSION STATEMENT

To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

UHY LLP Certified Public Accountants

Mitigating the Risks

- Third Party Audit
  - SAS 70 is dead, long live SOC

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Mitigating the Risks

New standards for third party audits

- SOC 1 – SSAE 16 – intended for services with relevance to ICFR
- SOC 2 – based on pre-defined controls "principles":
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- SOC 3 – Condensed and abbreviated SOC 2 report
  - Includes auditor opinion and Management's assertion
  - AICPA seal can be displayed
  - General availability

UHY LLP
Certified Public Accountants

New Standards

SOC Report Comparison

	Who Are the Users	Why	What
SOC 1℠	Users' controller's office and user auditors	Audits of f/s	Controls relevant to user financial reporting
SOC 2℠	Management Regulators Others	GRC programs Oversight Due diligence	Concerns regarding security, availability, processing integrity, confidentiality or privacy
SOC 3℠	Any users with need for confidence in service organization's controls	Marketing purposes; detail not needed	Seal and easy-to-read report on controls

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

When to use SOC 1, 2, 3

Will report be used by your customers and their auditors to plan/perform an audit of their financial statements?	Yes	SOC 1℠ Report
Will report be used by customers/stakeholders to gain confidence and place trust in a service organization's system?	Yes	SOC 2℠ or SOC 3℠ Report
Do you need to make report generally available or seal?	Yes	SOC 3℠ Report

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SOC 2 and 3 Criteria

	Trust Services Audit Framework					
	Area	Security	Availability	Integrity	Confident	Privacy
0.0	Common Controls					
1.0	Policies: The entity defines and documents its policies for the security, availability, processing integrity, and confidentiality of its system.					
1.1	The entity's policies for system security, availability, system integrity, and confidentiality are established and ……	þ	þ	þ	þ	N/A
1.2	The entity's system security, availability, system integrity, and confidentiality policies include, but may not be limited to ……					
2	Communications: The entity communicates its defined policies to responsible parties and authorized users					
2.1	The entity has prepared an objective description of the system and its boundaries and ……	þ	þ	þ	þ	N/A
2.2	The system security, availability, system integrity, and confidentiality and related security obligations are communicated	þ	þ	þ	þ	N/A
3	Procedures: The entity placed in operation procedures to achieve its documented system security, availability, system integrity, and confidentiality objectives in accordance with its defined policies.					
3.1	Procedures exist to……	þ	þ	þ	þ	N/A
3.2	Procedures exist to restrict logical access to the defined system including ……					N/A
4	Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security, availability, system integrity, and confidentiality policies.					
4.1	The entity's system security, availability, system integrity, and confidentiality is periodically reviewed and ……	þ	þ	þ	þ	N/A
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability……	þ	þ	þ	þ	N/A
	NOTE: Privacy criteria are described in AICPA publication "Generally Accepted Privacy Principles"					

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SOC 2 and 3 Criteria

- Over 120 individual controls criteria
- Focused on 4 key areas:
  - Policies
  - Communication
  - Procedures
  - Monitoring

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- You utilize a third party colocation facility for financial systems
- Which SOC report should you request?

(you may ask additional questions to get additional information)

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- You utilize a third party colocation facility for financial systems
- Which SOC report should you request?

- SOC 2 or SOC 3

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a third party SaaS provider for financial systems
- Which SOC report should you request?

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a third party SaaS provider for financial systems
- Which SOC report should you request?

- SOC 1 (SSAE 16)

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a public cloud provider for development and testing of financial systems
- Which SOC report should you request?

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a public cloud provider for development and testing of financial systems
- Which SOC report should you request?

- SOC 2 or N/A

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Additional Resources

- https://cloudsecurityalliance.org/
- http://www.aicpa.org/SOC/
- http://www.isaca.org

Questions?

David Barton, Principal
UHY LLP

Five Concourse Parkway
Suite 2430
Atlanta, GA 30328

678-602-4490

THE NEXT LEVEL OF SERVICE