TRANSFORMATION • SYNERGY • EXCELLENCE

The Increasingly Risky Business of Cloud Adoption

COMMIT.
BEST IN CLASS

CULTURE & UNITY • LEADERSHIP & ACCOUNTABILITY • INNOVATION • MARKET PROMINENCE • BEST IN CLASS

BDO

With You Today…

Jamey Loupe
Senior Manager, IT Audit
Risk Advisory Services

jloupe@bdo.com
713-960-1706

Learning Objectives

At the conclusion of this program, participants will be able to:

- Explain what the cloud is and basics of how it works;
- Describe the migration of IT infrastructure, applications and security to the cloud;
- Describe what cloud services are leading the industry;
- Identify the risks and benefits of migrating to the cloud; and
- Describe basic procedures for auditing the cloud.

What and Where is THE CLOUD?

Is The Cloud a Mystery?

What is The Cloud?

- The Cloud is a collection of servers and networks used to host data and applications.
- Exactly what functionality does The Cloud offer?
- SaaS, IaaS, PaaS, and XaaS….

SaaS – Software as a Service

SaaS is access to an application over the Internet. It is usually delivered to the user via a web browser. The user generally has limited administrator rights. Users responsibilities are covered under an SSAE18 - User Control Considerations or End User Considerations (UCC/EUC). More about SSAE18 later.

Storage	Enterprise Applications
• Google Drive • DropBox • MS OneDrive • iCloud • Pixl • Etc., etc., etc.	• ADP • Concur • Office 365 • Dynamics AX • Etc., etc.

IaaS - Infrastructure as a Service

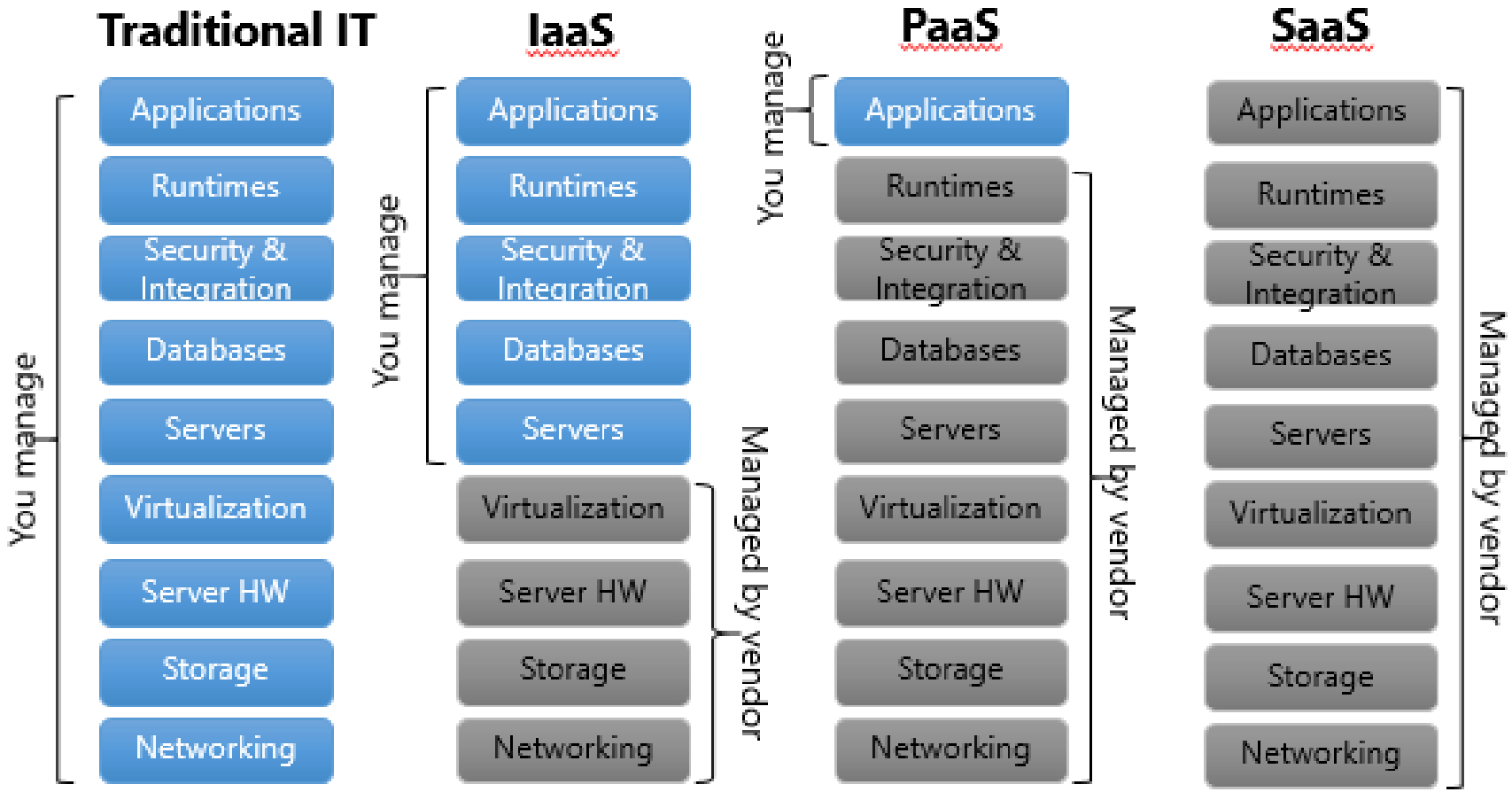
IaaS is a virtual machine or hardware built on a web platform. The end user is responsible for all the administrative tasks of the server (minus hardware) and all installed software. SSAE18 agreements usually with the web platform provider.

VMs	Security	Others
• Linux • Windows • iOS	• Firewalls • Monitoring Tools • Identity and Access Management • Encryption Management • Etc, etc., etc.	• Netscalers • Domain Controller • Active Directory Federated Services • Blob Storage • Etc, etc., etc.

PaaS – Platform as a Service

PaaS is a bundle of software and server with operating system sold to the end user. End user gets a box and software to do with what they want. Vendor manages OS and all back end administrative functions of the hardware. PaaS is generally built on IaaS. PaaS is used heavily for development and test environments.

Cloud Functionality



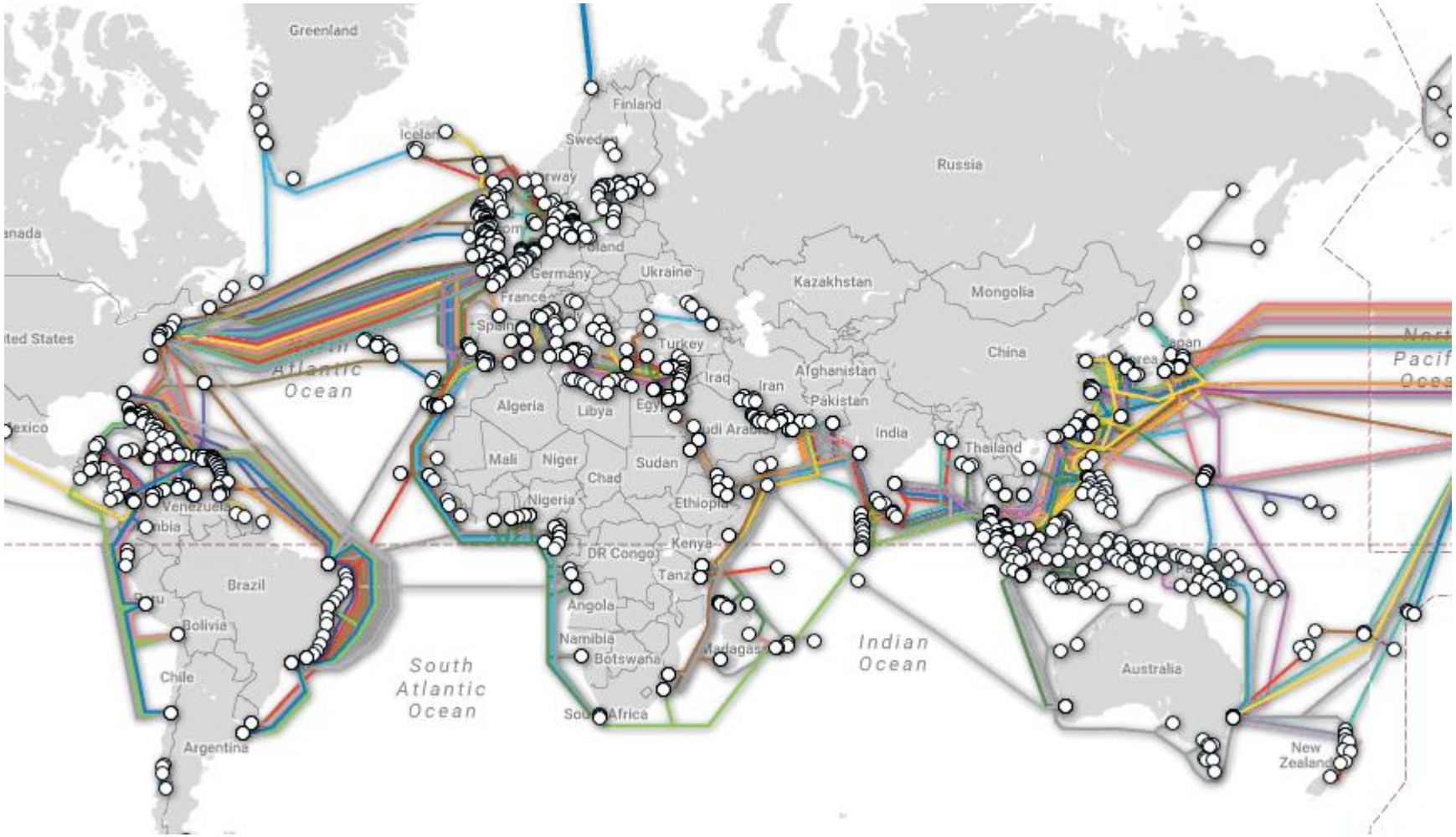
XaaS?....

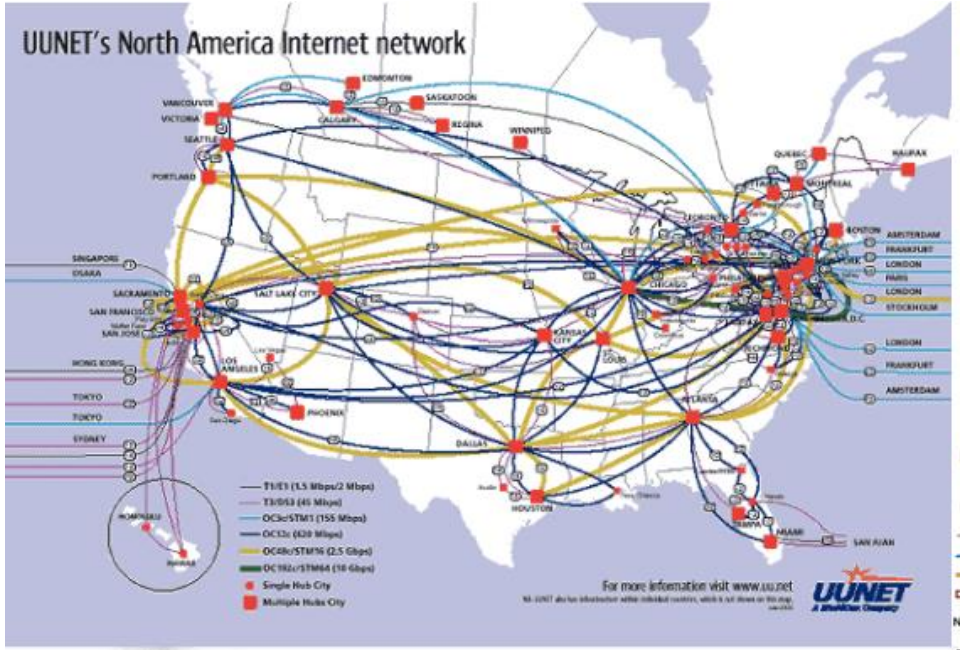
XaaS - Everything as a Service

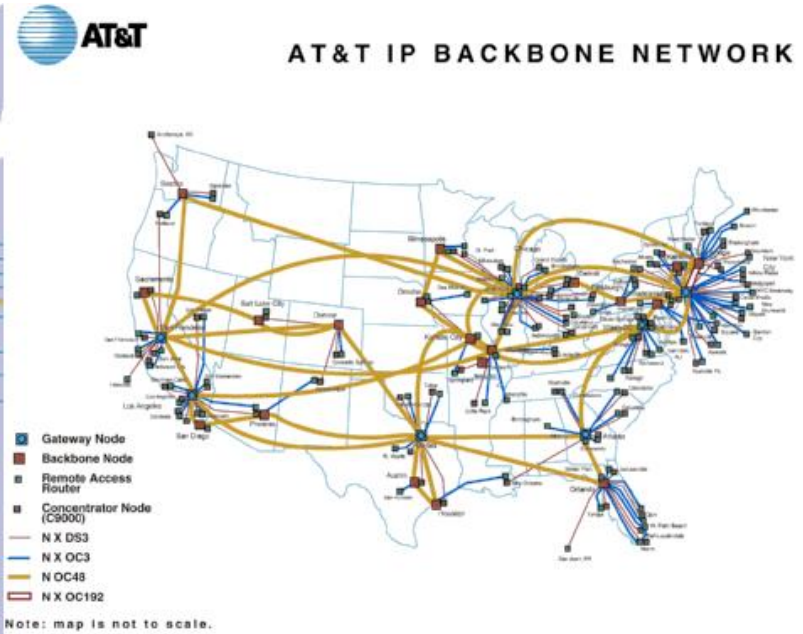
XaaS is the future of the cloud and everyday life.

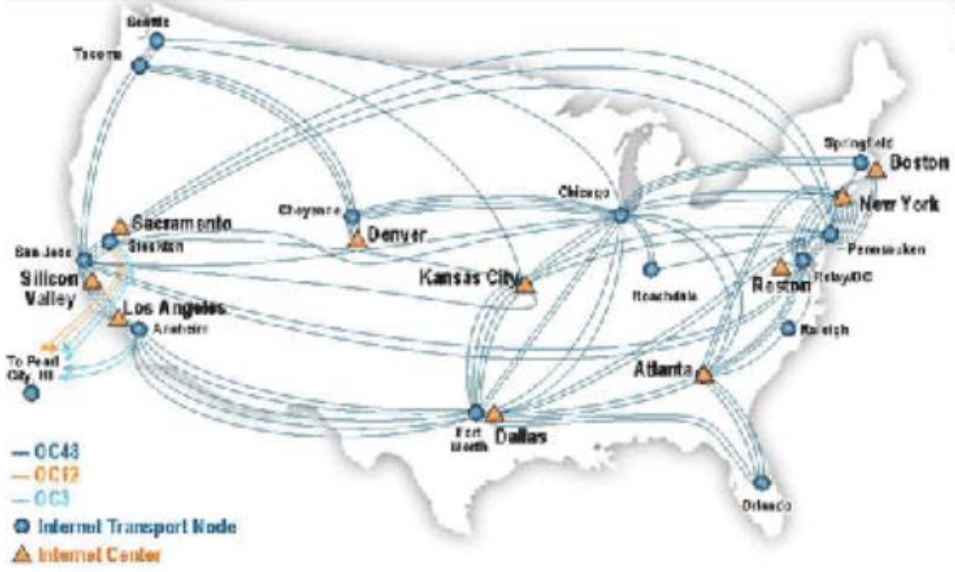
The idea is that as cloud services mature everything will be offered as a service. (e.g Grocery as a Service, Restaurants as a Service, Delivery as a Service, Business Process as a Service, etc.)

Backbone of The Cloud (aka the Internet)




UUNET's North America Internet network
For more information visit www.uu.net
UUNET


AT&T
AT&T IP BACKBONE NETWORK
Gateway Node
Backbone Node
Remote Access Router
Concentrator Node (C9000)
N X DS3
N X OC3
N OC48
N X OC192
Note: map is not to scale.


Boston
New York
Sacramento
Denver
Kansas City
Silicon Valley
Los Angeles
Atlanta
Dallas
OC48
OC12
OC3
Internet Transport Node
Internet Center
Sprint.


Level(3)
COMMUNICATIONS
Seattle
Portland
Oakland
San Jose
Sacramento
San Francisco
Salt Lake City
Denver
Omaha
Chicago
Detroit
Cleveland
Buffalo
Albany
Pittsburgh
Indianapolis
Cincinnati
Louisville
St. Louis
Kansas City
Richmond
Raleigh
Charlotte
Nashville
Memphis
Atlanta
Las Vegas
San Luis Obispo
Los Angeles
Orange
San Diego
Phoenix
Dallas
Fort Worth
El Paso
Austin
San Antonio
Houston
New Orleans
Tampa
Orlando
Jacksonville
Miami
Manchester
Boston
Providence
Hartford
Stamford
Long Island
New York City
Jersey City
Newark
Princeton
Philadelphia
Baltimore
Wilmington
Washington, D.C.

Cloud Providers

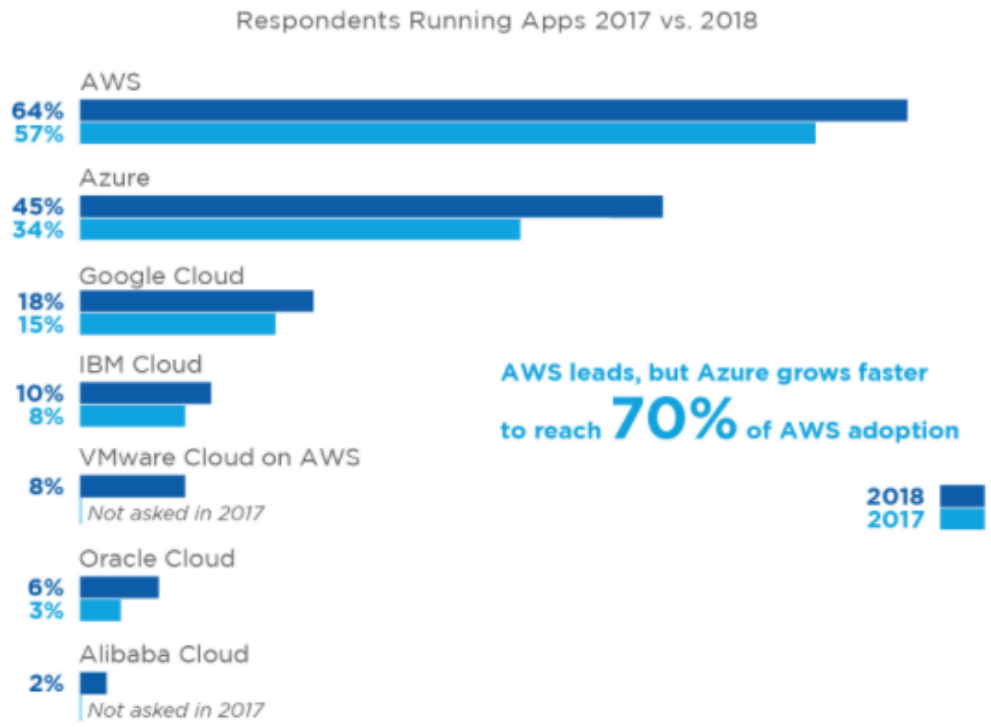
Top Cloud Providers

Top Cloud Providers

Area	AWS	Azure	Google	IBM
% Adoption	68%	58%	19%	15%
YoY Growth in Adoption	15%	35%	26%	50%
% Adoption in Beginners	47%	49%	18%	14%
% with Footprint > 50 VMs	58%	44%	17%	14%
YoY Growth in Footprint > 50 VMs	14%	38%	42%	56%

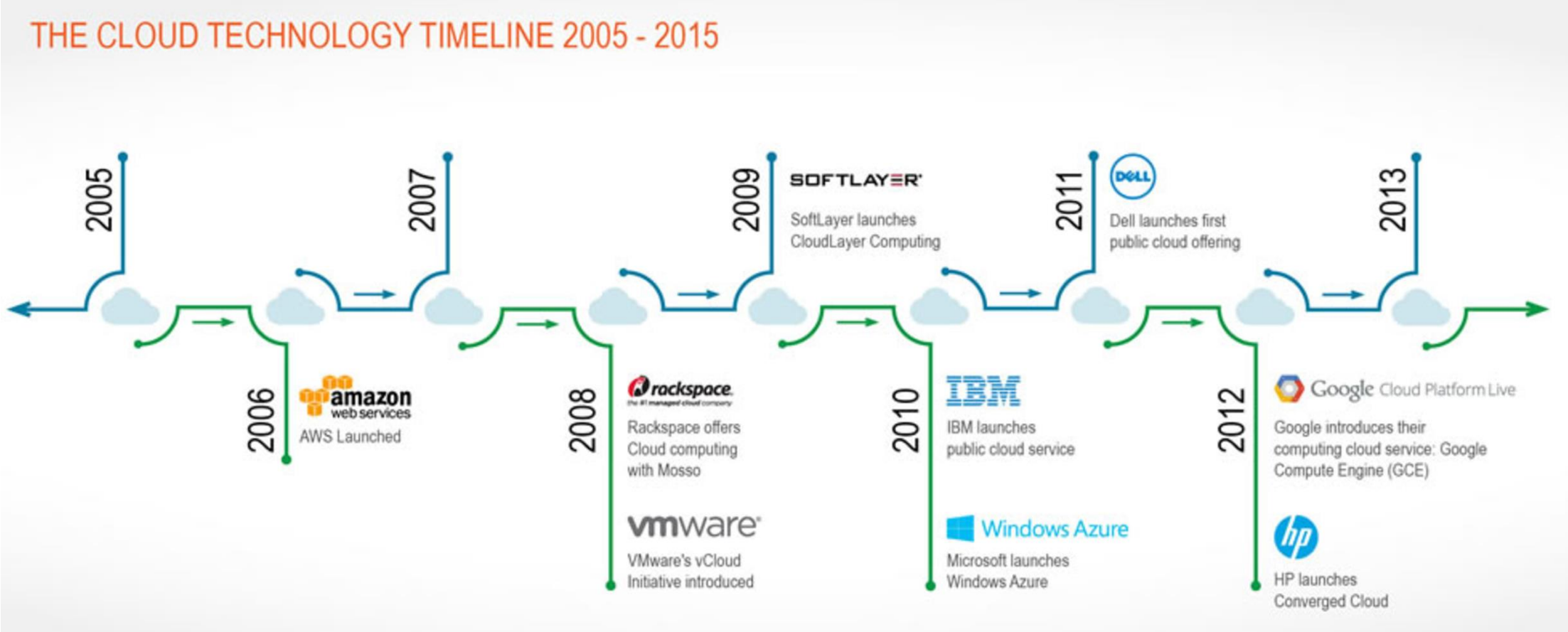
AWS leads *Other vendors lead*

Source: RightScale 2018 State of the Cloud Report

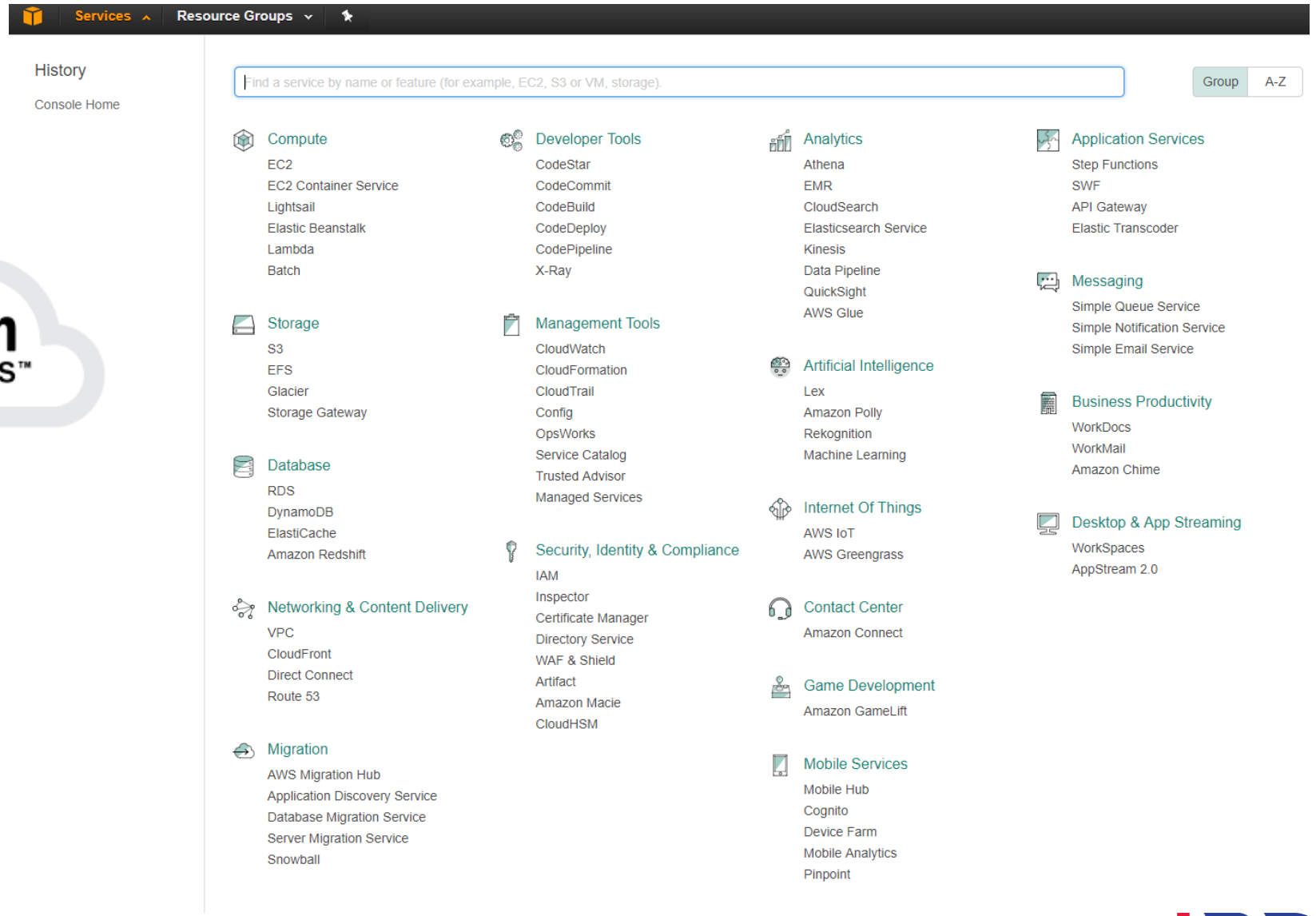


Source: RightScale 2018 State of the Cloud Report

Evolution of The Cloud



AWS Overview



Microsoft Azure Overview

Offers free account with $200 of credit at https://portal.azure.com/

Concerns of The Cloud

- Security
- Multi-Tenancy vs Single Tenancy
- Data Ownership
- Cross border laws
- Privacy
- Governance
- Rogue Cloud Applications

Cloud v. On Premise

CLOUD	ON PREMISE
Security	Yes
Compromised passwords	Yes
Multi-tenancy vs single tenancy	No
Data ownership	No
Cross border laws	No
Privacy	Yes
Governance	Yes
Rogue cloud applications	Yes

Other On Premise Concerns

SHARED WITH THE CLOUD

- Security
- Cross border laws
- Privacy
- Governance
- Rogue Cloud Applications

ON PREMISE

- Disaster Recovery
- Physical Security
- Data Center space
- Environmental Controls
- Lease renewals
- Hardware obsolescence
- Hardware disposal

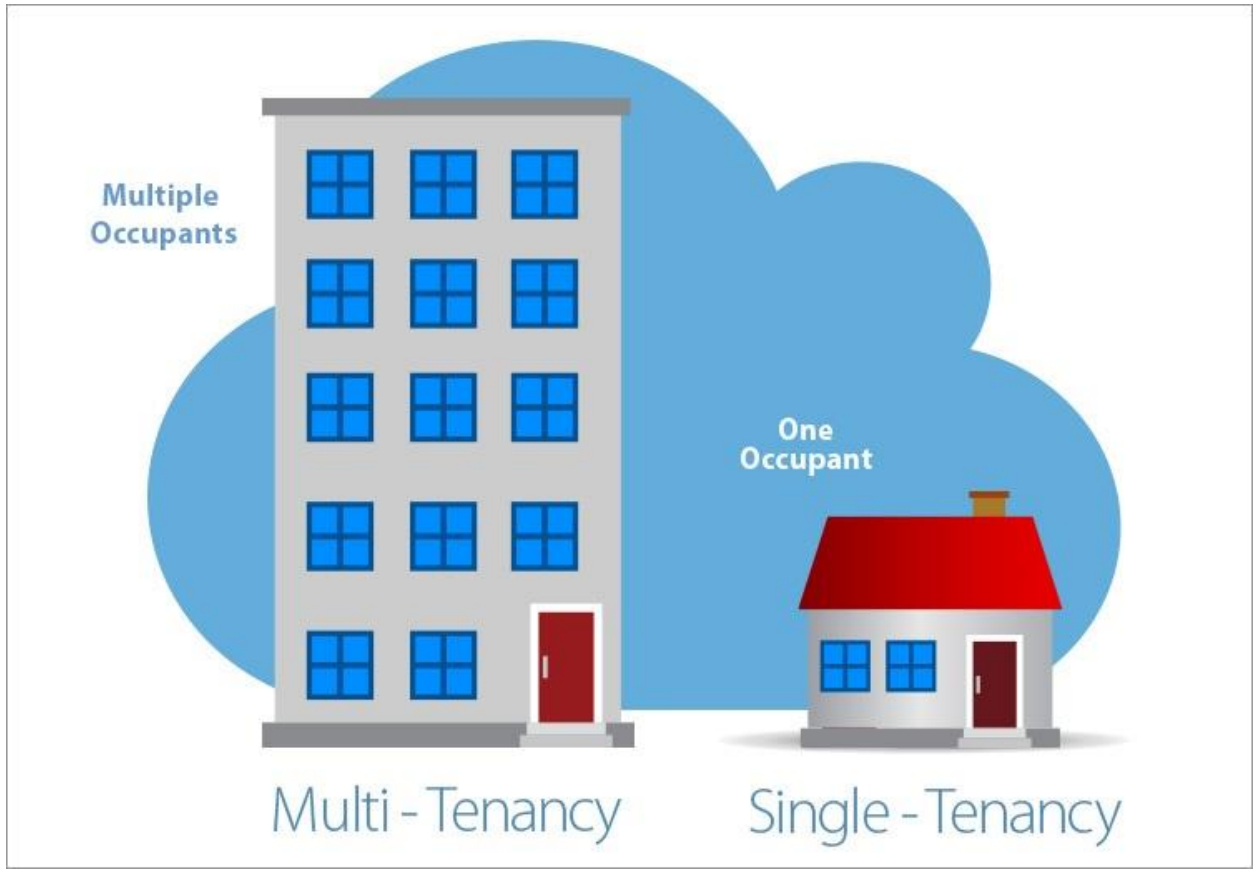
Security of The Cloud

The only way to ensure the complete security of data is to have no users.

Top cloud vendors have built in security features that strengthen the security in their environments.

- Built in fragmentation and encryption
- Built in Redundancy
- Built In Detection and Monitoring
  - Power BI included in Microsoft Azure to monitor security and availability
  - AWS Cloudwatch
- Fully staffed 24X7 Security Operations Center (SOC)
- Ability to build in further security applications and monitoring
  - Cloud Access Security Broker (CASB)
  - Cloud Firewall/Proxy
  - Just In Time Virtual Machine

Multi-Tenancy v. Single Tenant



Risk of another tenant gaining access to company data.

Risk addressed through partitioning and encryption.

Single tenancy significantly raises the cost.

Data Ownership

It is crucial that organizations specify that all data created by individuals of the organization belongs to the organization and will be provided to the organization upon termination of the contract.

The most critical question companies have to ask themselves when considering a cloud service is “Who owns the data?” With regard to data ownership, there are two types of data:

1. Data created by the user prior to uploading to the cloud.
   a. This data can be protected by copyright laws and is owned by the creator.

2. Data created on The Cloud platform.
   a. This data could be owned by anyone depending on the terms of the contract between the cloud vendor and the user.

Benefits of Moving to The Cloud

There are numerous benefits of cloud computing over on premise solutions:

- Flexibility
- Scalability
- Ease of Disaster Recovery
- Automatic updates to software
- Access data from anywhere
- Improved control of documents
- Improved collaboration
- Cost*
- Security**

* Improving cost requires businesses to manage cloud usage and turn off servers as they are not in use.
** I have security as a benefit as the cloud offers added security benefits that I mentioned earlier.

Auditing The Cloud

Addressing Risks of The Cloud - Policies

Is Cloud Computing included in the scope of your organization's IT policies?

- Define Cloud Computing in your organization – "the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
- Microsoft's definition of Cloud computing – "Simply put, cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, and more—over the Internet ("The Cloud").
- Cloud Security Alliance - 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).

Addressing Risks of The Cloud, cont'd.

Other items that should be addressed in policies:

- Who is responsible for authorizing the acquisition and use of Cloud Computing services in your organization, i.e. IT, Procurement, Legal or Other?
- Policy should identify who is responsible for reviewing the "terms of service" for Cloud Computing solutions, e.g. Data Ownership.
- Does the use of third party Cloud Computing services comply with your organization's existing policies, i.e. Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/BYOD Policy and all laws and regulations governing the handling of personally identifiable information (PII), corporate financial data or any other data owned or collected by your organization?

Addressing Risks of The Cloud, cont'd.

Other items that should be addressed in policies:

- Who decides what data may or may not be stored in The Cloud?
- Can personal cloud service accounts be used to store, manipulate or exchange of your organization-related communications or organization-owned data?
- Are there pre-approved Cloud Computing services in your organization? If so, you may want to list them
- How is onboarding of Cloud Computing services managed?

Evolution ➔ SAS 70 vs SSAE 16

Figure 2—SAS 70 vs. SSAE 16[10]		
Issue	**SAS 70**	**SSAE 16**
Focus	ICFR	ICFR (not technically different)
Basis	Management's choice	Risk basis for controls implemented/chosen
Period	Specific point in time: close	System description covers entire period of testing
Assertion	Audit	Attest
Management	Not applicable	Management's written assertion
Use	Basically, the public	User auditor, management of SO, management of user

Evolution → SSAE 16 → SSAE 18

- In April 2016, the American Institute of Certified Public Accountants' (AICPA) Auditing Standards Board (ASB) completed its Clarity Project issuing Statement on Standards for Attestation Engagements (SSAE) 18, Attestation Standards: Clarification and Recodification.
- Accordingly, SSAE 18 supersedes the existing standards under which a SOC report is issued, namely AT 801 (SOC 1) and AT 101 (SOC 2 or SOC 3), and is effective for SOC 1, SOC 2, and SOC 3 reports dated on or after May 1, 2017.
- SSAE 18 does not represent a major overhaul of the existing attestation standard; it is a clarification and recodification. For the most part, the new standard is intended to remove any ambiguity from established guidance that practitioners already should be following.

Evolution ➔ SSAE 16 ➔ SSAE 18

SSAE 18 Changes

Introduces the concept of *"complementary subservice organization controls"* (CSOCs)
The new term defines controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

Similar to CUECs, service organizations should carefully consider and identify CSOCs that are necessary to help achieve the control objectives in the SOC report, including the controls at the service organization that monitor the effectiveness of controls at the subservice organization. When CSOCs have been identified by the service organization, they will be handled similarly to CUECs in the scope paragraph of service auditor report when using the carve-out method.

SOC Framework

Figure 1—SOC Framework			
Applicable...	**SOC-1**	**SOC-2**	**SOC-3**
Standard	SSAE 16: AICPA Guide (2011)	AT 101: AICPA Guide (2011)	AT 101: Technical Practice Aid
Controls	ICFR	Security/ Systems, Privacy	Security/ Systems, Privacy
Controls reference	Undefined	Trust Services Principles[7]/ GAPP[8]	Trust Services Principles/ GAPP
Usage of report	User auditor, management of SO, management of user	Knowledgeable parties (see AT 101)	Anyone

Using SOC Reports to Evaluate Cloud Service Providers

- A 2017 presentation at the RSA Conference included a survey that reported 48% of respondents found that a SOC 2 report was the most effective way to assess cloud provider risk.
- How can enterprises use SOC 2 to evaluate cloud providers, and is it really the most effective method?
- Definition of SOC 2® - These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

SOC Reports

- A SOC 1 report is for service organizations that impact or may impact their clients' financial reporting. – Basically if it will be SOX relevant if it is a publicly traded company. SOC 1 lists the ITGCs and other controls needed for company's using their software.
- A SOC 2 report is for service organizations that hold, store or process information of their clients, but is not significant to financial reporting (e.g., would not affect their income statement or balance sheet). Distribution is limited to knowledgeable parties.
- A SOC 3 report is designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2® Report. Because they are general use reports, SOC 3® reports can be freely distributed.

SOC Report Types

- Type 1: A design of controls report. This option evaluates and reports on the design of controls put into operation as of a point in time.
- Type 2: Includes the design and testing of controls to report on the operational effectiveness of controls over a period of time (typically six months).
- Pertains to SOC 1 and SOC 2 reports

Why a SOC 2 Type 2 Report?

- Focused on Service Providers versus Financial Controls
- It is Prescriptive vs. Descriptive
- Built around Trust Service Criteria (TSC)
  - Five principles include: Security, Availability, Processing Integrity, Confidentiality and Privacy
- SOC 2+ ➔ When a service organization wants a report on both the trust services principles and the additional criteria—such as the HITRUST CSF, the Cloud Controls Matrix from the Cloud Security Alliance, etc.—a SOC 2+ report is an option.

Example of Complementary User Entity Controls (CUEC)

COMPLEMENTARY USER ENTITY CONTROLS

ADP controls were designed with the assumption that certain controls would be implemented by user entities (clients). It is not feasible for control objectives relating to transaction processing to be achieved completely by ADP's management or the user entities acting alone. It is necessary for user entities to implement controls to achieve some of the control objectives identified in this report (as applicable).

The User Entity Control Considerations presented below are controls that user entities should have placed in operation to achieve the control objectives in this report and should not be regarded as a comprehensive list of controls that should be used by user entities. The applicability and implementation of these controls may vary by user entity based on the nature of the services and applications being used by ADP's user entities. Other controls may be required by user entities and should therefore be evaluated by the user entity. User entity auditors should consider whether user entities have implemented these controls (as applicable) when understanding and evaluating the internal controls at the respective user entity.

Trust Services Criteria (TSC)

The TSC are classified into the following categories:

- Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- Availability. Information and systems are available for operation and use to meet the entity's objectives.
- Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- Confidentiality. Information designated as confidential is protected to meet the entity's objectives.
- Privacy. Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Benefits of SOC for Cloud Providers

Undertaking SOC attestation can provide numerous benefits, including:

- Building trust with current customers and prospects. SOC reports can also be a factor in the RFP process—some companies demand them as a condition of participating.
- Providing a look under the hood without requiring the user entity to perform the audit itself.
- Precludes having to audit partner organizations (hundreds or even thousands of outside service providers) one-by-one, which would be time-consuming, inefficient and disruptive to both parties.
- Provides peace of mind about whether the controls are functioning as expected, and how they can be improved.
- SOC 2 can prove useful in organizational and regulatory oversight, vendor management, and governance and risk management endeavors.

Evaluating Cloud Computing Risk

- Use SOC2 report to get approximately 80% coverage of Cloud Computing risk evaluation
- Use other tools, such as the following Cloud Security Alliance (CSA) free tools
  - Cloud Controls Matrix (CCM) version 3.01 as of 10/06/2016:
    - ✓ contained 133 controls cross referenced to 34 standards/frameworks
  - Consensus Assessments Initiative Questionnaire (CAIQ) version 3.0.1 as of 12/05/2016:
    - ✓ contained 179 controls cross referenced to 3 standards/frameworks

Question

What stage is your organization at in adopting cloud services?

A. Running some applications but majority of servers still on premise/hosted.
B. Majority in the cloud with few servers on premise/hosted.
C. Haven't even started thinking about moving to the cloud.

Conclusion

Jamey Loupe
Senior Manager, IT Audit
Risk Advisory Services

jloupe@bdo.com
713-960-1706