

Auditing Your Cloud Computing Service Provider – Critical Questions to Ask

September 16, 2011

Allen Lum

Director Information
Technology & Security

Thomas Daggett

Director Internal Audit &
Risk Management Practice



Agenda

Introduction

Cloud Computing Foundation

Growth of Cloud Computing

Questions to Ask of a Service Provider

Q&A

Setting the Stage...

- **Introduction**
- **Cloud Computing Foundation**
- **Growth of Cloud Computing**
- **Questions to Ask of a Service Provider**
- **Q&A**
- **Tom Daggett,**
Cloud Foundation; Benefits and Drawbacks;
Considerations and Risks
- **Allen Lum,**
Questions to Ask Your Cloud Provider

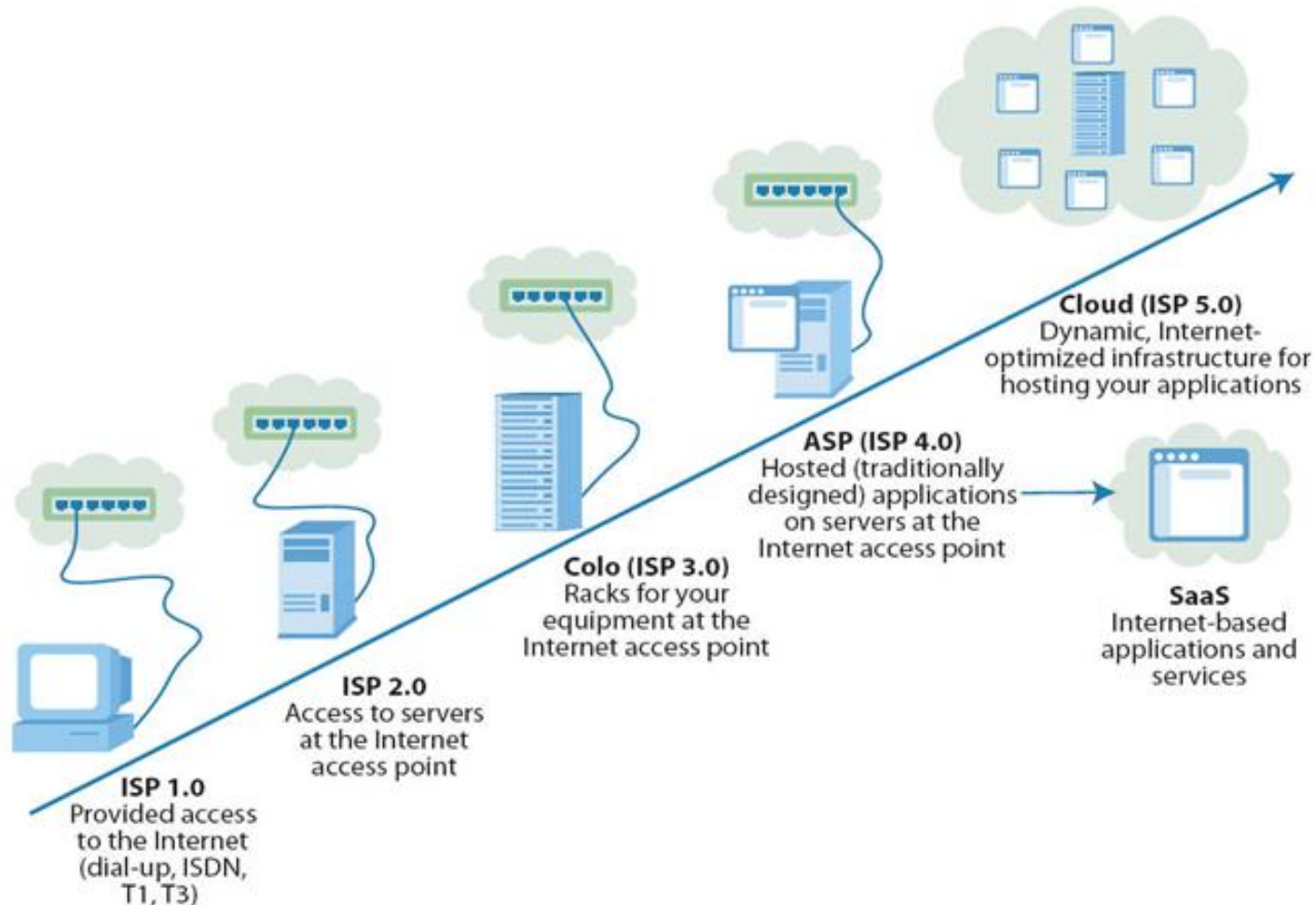
Cloud Computing Foundation

What is Cloud Computing?
Different Types of Cloud Computing

History of the Cloud

The term "cloud" is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents.

Evolution of Computing

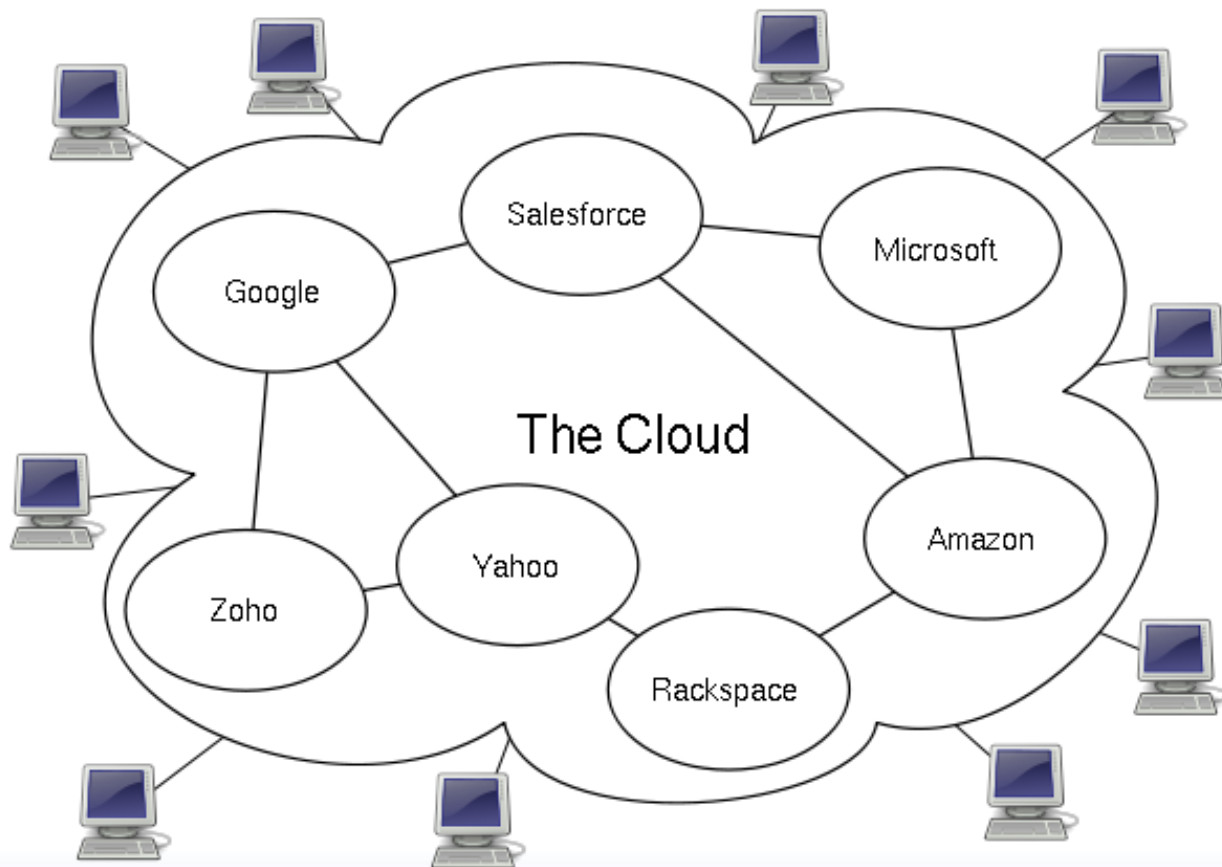


Evolution of Computing

- ❑ In simple terms
- ❑ Specific Applications
- ❑ The Cloud Model
- ❑ 360 degrees from Dumb Terminals

Cloud Computing

Cloud computing refers to the provision of computational resources on demand via a [computer network](#).



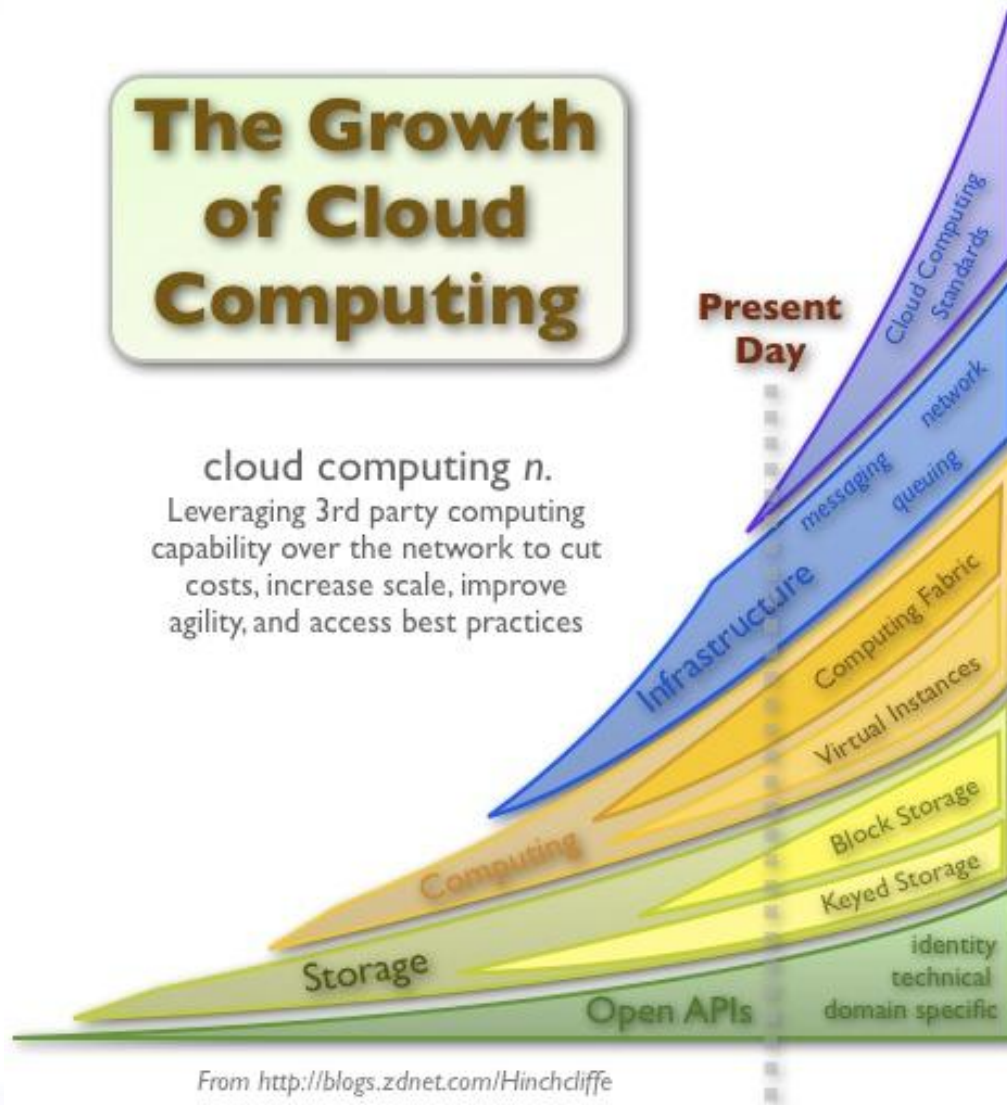
Cloud Movement

- ❑ **Cloud-based IT services have been enjoying extraordinary momentum in recent years.**
- ❑ **IDC (International Data Corporation) Prediction**
- ❑ **Private Network to Cloud**

Growth of Cloud Computing

The Growth of Cloud Computing

cloud computing *n.*
Leveraging 3rd party computing capability over the network to cut costs, increase scale, improve agility, and access best practices



From <http://blogs.zdnet.com/Hinchcliffe>

Cloud Movement



POTS, PANS and SANs
Intelligent Network (IN)



Internet + Virtualization
= Cloud



Intelligent Collaborating Cloud
Network (ICCN)



The Past



The Present



The Future???

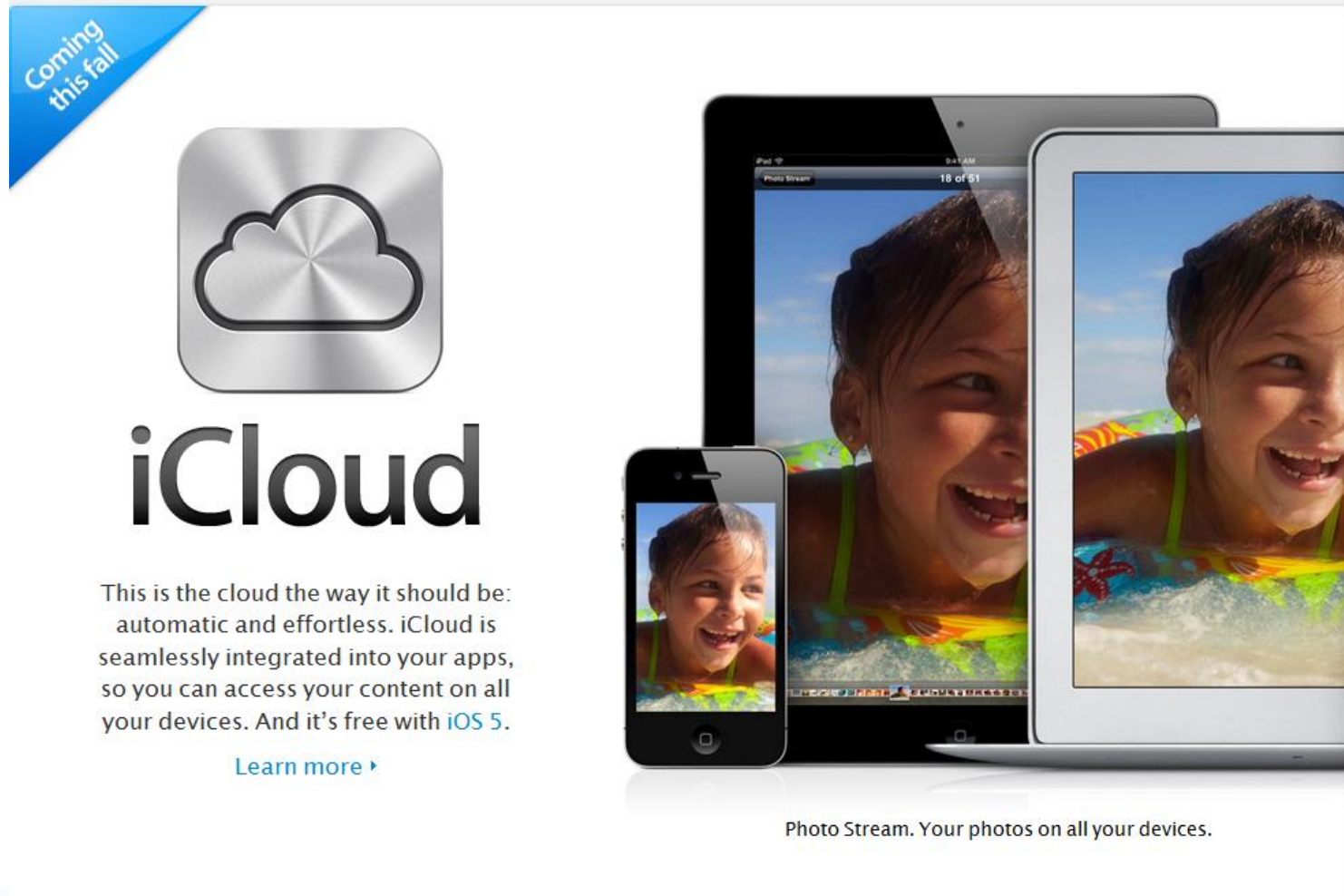
Integration of Services into the Cloud: Salesforce Service Cloud



From Search to Cloud



Apple – The Game Changer?



Coming this fall

iCloud

This is the cloud the way it should be: automatic and effortless. iCloud is seamlessly integrated into your apps, so you can access your content on all your devices. And it's free with iOS 5.

[Learn more >](#)

Photo Stream. Your photos on all your devices.

From Books to the Cloud

amazon cloud player



Buy Anywhere, Play Anywhere
And Keep All Your Music in One Place

Cloud Risk

- ✓ **What is Risk?**
 - Internal Audit's Role?
 - Risk Response
- **Risk (rsk) *n.* 1.** The possibility of suffering harm or loss; danger. **2.** A factor, thing, element, or course involving uncertain danger; a hazard: "the usual risks of the desert: rattlesnakes, the heat, and lack of water" (Frank Clancy).
- **COSO Definition** –“the possibility that an event will occur and adversely affect the achievement of an objective”

Cloud Risk

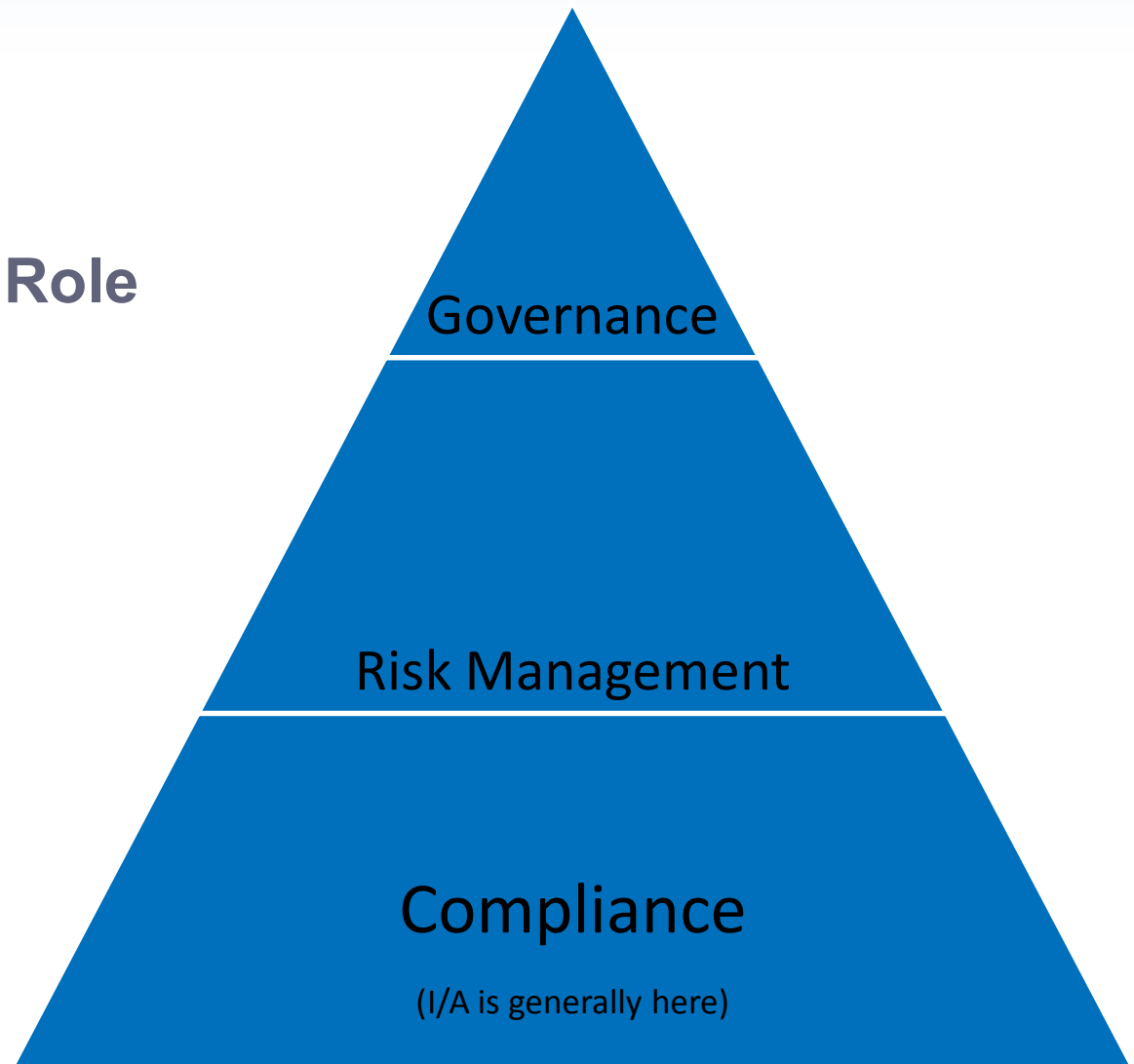
- ❑ **RISK** – The level of risk your company assumes

- ❑ **Risk Assessments** – You should now include your cloud usage

- ❑ **With Risk Comes the Benefit of the Cloud**

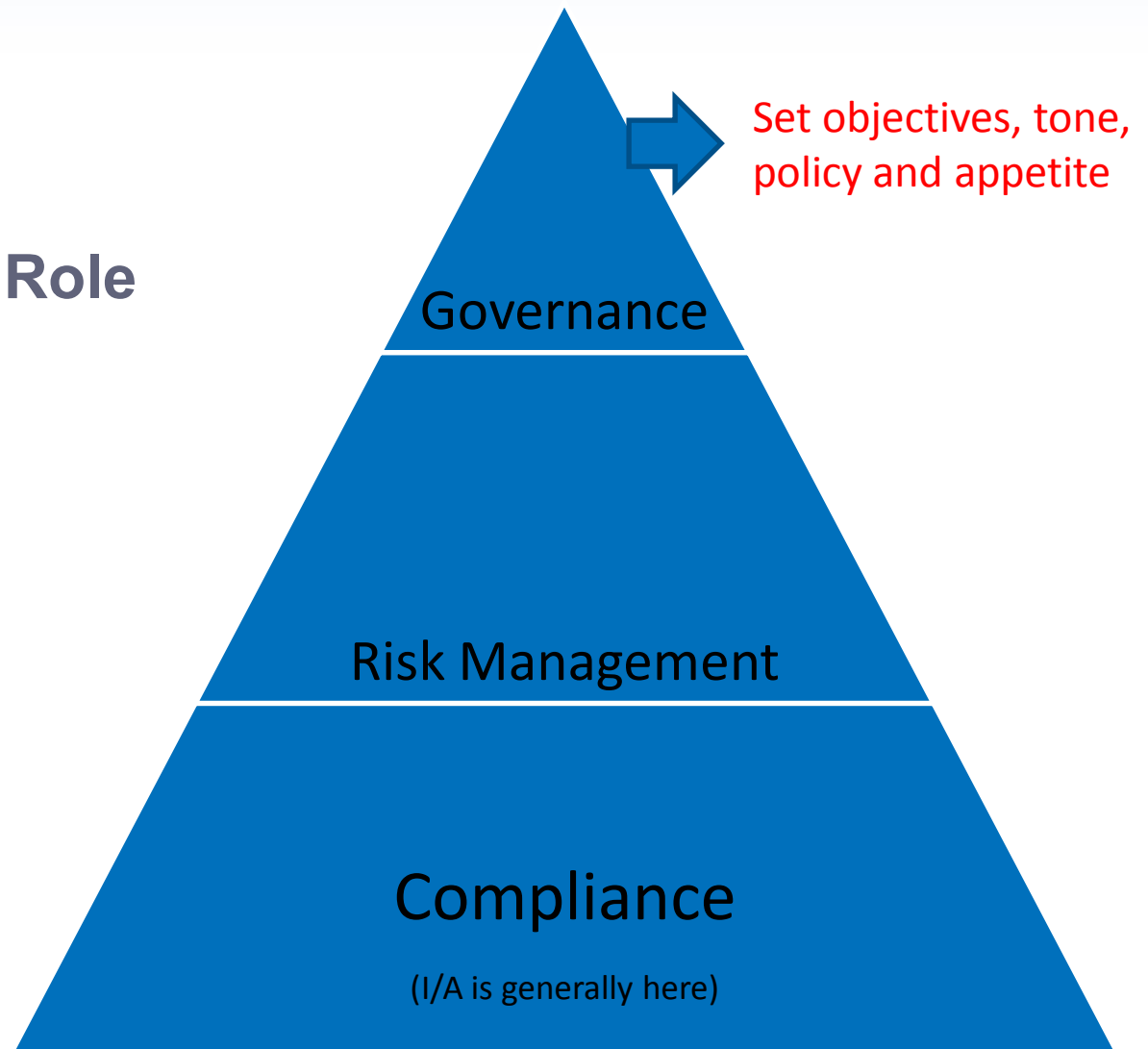
Cloud Risk

- Risk?
- ✓ **Internal Audit's Role**
- Risk Response



Cloud Risk

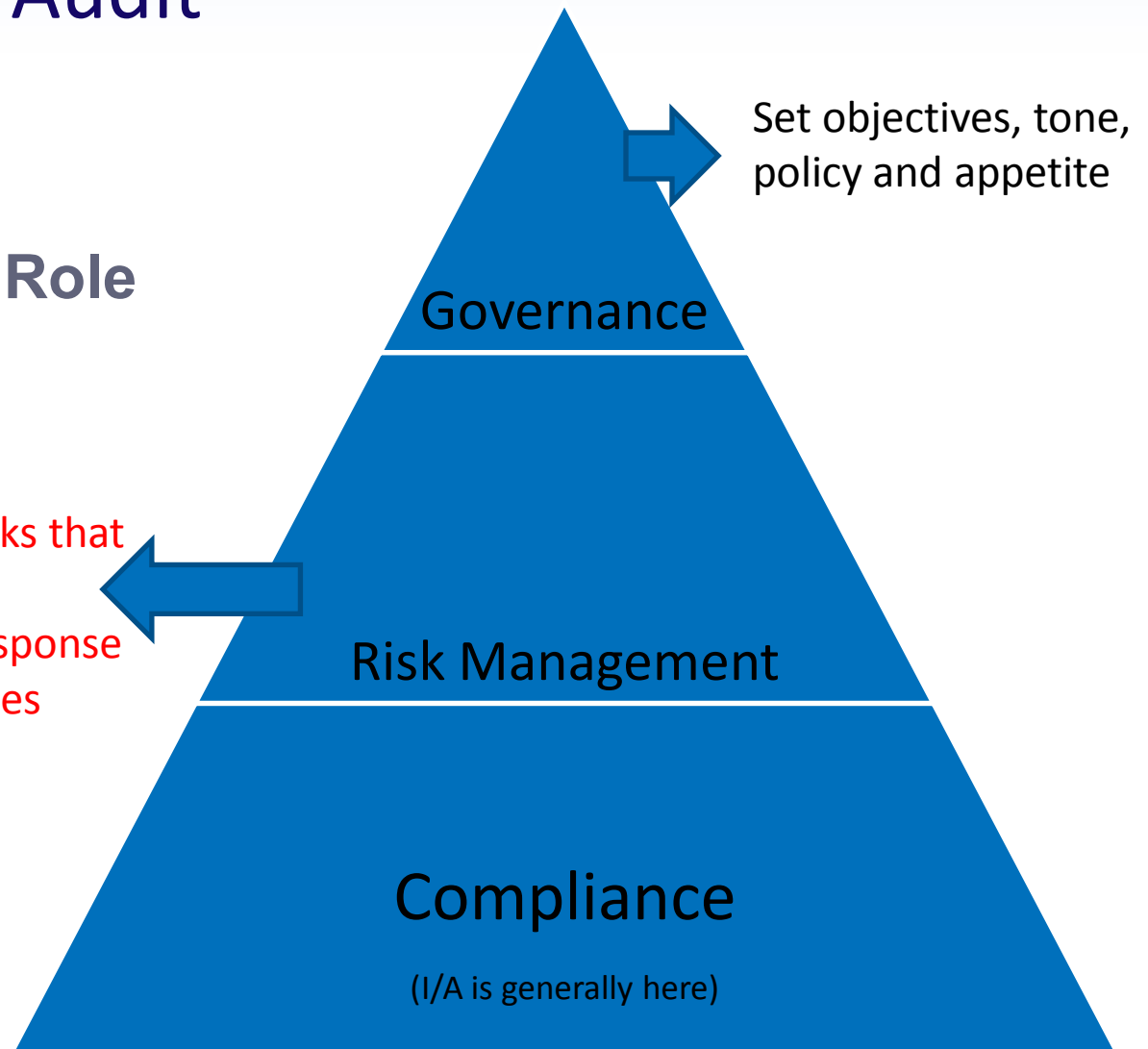
- Risk?
- ✓ **Internal Audit's Role**
- Risk Response



Risk & Internal Audit

- Risk?
- ✓ **Internal Audit's Role**
- Risk Response

Identify and Assess Cloud Risks that may affect ability to achieve objectives, determine risk response strategies and control activities

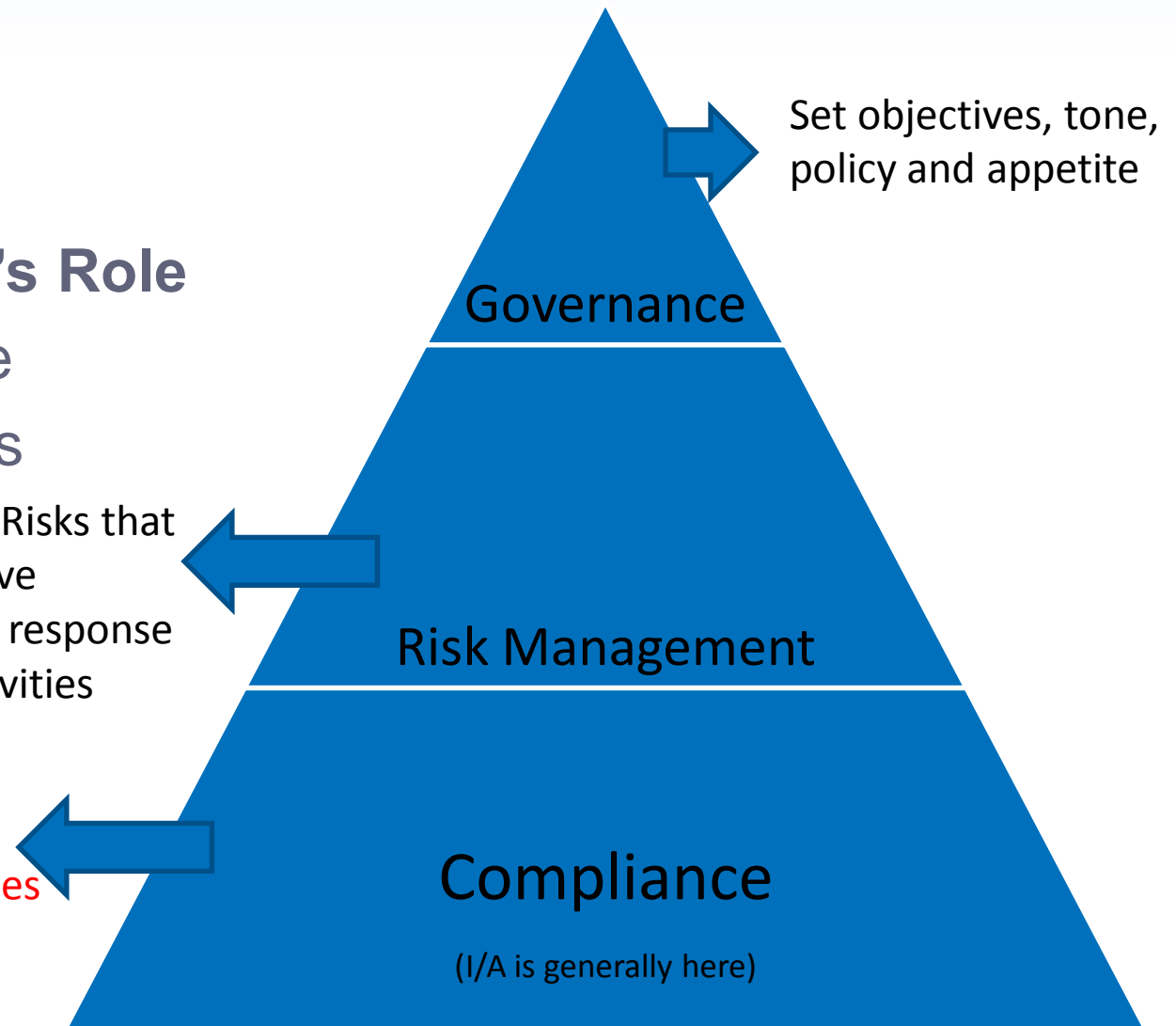


Cloud Risk

- Risk?
- ✓ **Internal Audit's Role**
- Risk Response
- Driving Returns

Identify and Assess Cloud Risks that may affect ability to achieve objectives, determine risk response strategies and control activities

Ensure adherence with objectives, laws and regulations, internal policies and procedures



Cloud Risk

- Risk?
- ✓ **Internal Audit's Role**
- Risk Response
- Compliance phase
- Testing
- Reporting
- Then you do it again next phase
- IA is uniquely positioned to positively impact operations and manage risk by considering the Cloud risk exposure

Cloud Risk

- Risk?
 - Internal Audit's Role
 - ✓ **Risk Response**
- Risk represents uncertainty
 - Risk success is based on an organization's ability to:
 - Recognize the onset of Risk
 - Adjust Risk Assessment and Audit Plan
 - Address Risk timely, effectively and with proper Asset Deployment

Cloud Risk & Internal Audit

- Risk?
 - Internal Audit's Role
 - ✓ Risk Response
- How do you properly assess Cloud Risk?
 - How do you prepare to be successful in your Risk Management?
 - Risk Readiness is the **RESPONSE** to Identified Risk



**To Mitigate Risk
Ask the Right Questions of Your Cloud Provider**

Decided to go to the Cloud? What now?

Questions to Ask Your Prospective Cloud Service
Provider to Mitigate Your Risk

Question 1

Who owns the Data once it gets into the Cloud?

Expected Provider Response – YOU DO!

- Your organization must insist, in your contract, on owning all IP Addresses, data or any other information/physical assets that may be in a cloud environment.
- Understand that there is a difference between:
 - Ownership of IP Addresses that allow the service provider to do their job.
 - Intellectual property or assets, such as data that is placed in the cloud.

Question 2

Will you be locked in with a Service Contract or can you avoid a lock-In?

Expected Provider Response - Usually Yes...but Money Talks!

Most Vendors will try to get you committed to the longest term contract possible, below are three possible solutions:

- 1) **Contractual Lock-In: i.e./ 5 year vs. month to month**
Solution – test before locking into a long term agreement
- 2) **Technical Lock-In: Proprietary APIs vs. Industry Standards** Solution – Avoid at all costs
- 3) **Inertial Lock-In: The solution works when implemented, there is no need for lock-in**
Solution – No one feels the need to be locked into any contract

Question 3

Are you SSAE 16 Type II Certified (formally SAS-70) or ISO27001?

Expected Provider Response - YES and the reports are available to you.

- SSAE 16 or ISO27XX does not equate to a Secure Environment!
- Ask questions as part of your due diligence. What parts are certified or in compliance?
- Each of the certifications require policies and procedures but are not specific on the type required.

Question 4

What Kind of Incident Monitoring and Logging is performed on the cloud systems? Is the process the vendor has the same, as though you were running the services on your organization's internal systems?

Expected Provider Response - We performed monitoring on the infrastructure and application level.

All events are logged and available for your review.

We have a detailed Incident Response Protocol/ Plan.

- Inquire if the reporting of anomalies is done in real time and that your organization will have unrestricted access to the log files.
- Confirm if the monitoring of multiple events is tied together.
- Follow-up on monitoring of cloud to cloud transfers.

Question 5

Do you have Third Parties perform Attack and Penetration Tests against the Infrastructure and Applications?

Expected Provider Response - Yes and these reports are available for your review.

- Examine the report and determine if there are any critical vulnerabilities that have been exploited. If so, determine whether management has taken corrective action to resolve the issues identified.

Question 6

How Secure Is My Data? Is Encryption Used?

Expected Provider Response - In our opinion, the provider should be encrypting data whenever possible – data at rest, in transit, etc.

- Recognize it is virtually impossible or cost prohibitive to have every piece of data 100% secure.
- Remember you are connected to the internet!
- You need to review the SSAE 16 or ISO certification reports that describe the data protection policies and procedures.

Question 7

How do I know you or anyone else is not gaining access to my data?

Expected Provider Response - We have implemented security policies and procedures that ensure no person will access your data without explicit permission. These policies and procedures have been audited and tested in our SSAE 16 Review.

- If you are using a multi tenant thirty party cloud, such as Amazon, it may be impossible and unrealistic to prevent all possible data access.



Question 7 (Cont)

Realize the difference between data access by system or programmed processes and access by human kind:

- System access is often required – back-ups, migrations to other devices, etc.
- Access by a system administrator (Human Kind is FORBIDDEN) and unacceptable.
- In order to keep data private, encrypt the data before sending it to the cloud.

Question 8

Are you compliant with all the various regulations – HIPAA/NIST/etc.?

Expected Provider Response - Using our services should not impact your HIPAA compliance.

- As the service provider is typically not a healthcare or financial services organization, the question should be:
“If I utilize your services will it impact my compliance with HIPAA?”

Question 9

How effective is your Disaster Recovery Program?

Are your Disaster Recovery Plans Tested?

Expected Provider Response - Yes, here is a copy of the Disaster Recovery and back-up test results.

- Review the current SSAE-16 for results on Disaster Recovery Testing.

Question 10

What is your uptime history of your Network and Major systems Components ?

Expected Provider Response - Here are availability reports and statistics showing the uptime and availability of our major Cloud resources.

- Just ask them for the reports. These reports should cover at least the last 6 months at a minimum and should be 99 to 100% uptime.

Question 11

How much notice do I need to give you to terminate or expand my use of services?

Expected Provider Response - No time at all, or very close.

- It is required that your cloud provider enable elasticity – near real time at worst case scenario.
- Old School vs. Cloud: If a service provider requires extensive set up time and advance pre-work to scale you up or down, they are not a true cloud service provider.

Question 12

How do I know that I am realizing efficiencies by moving to the cloud?

Expected Provider Response - Let me show you.

If the return on your investment of saving is not there you should not be going to the cloud. In addition to the initial capital costs you should be including:

- Man hours for conversion to the cloud
- Additional Security Costs
- Opportunity Costs of Capital

Question 13

What type of forensics tools are available for use in the event of a breach or data recovery request?

Expected Provider Response - A specific protocol has been established for the protection and retrieval of electronic evidence. Tools are available for recovery data and analysis.

- Understand the jurisdictional and legal ramifications pertaining to the physical location of the cloud systems holding data under investigation.

Question 14

What happens if my company should discontinue your services?

Expected Provider Response - Your data will be removed from our system, we will provide a proper migration path to any format that you desire.

- What is the exit strategy should the cloud service provider not work out or they go under?
- Areas to consider:
 - Where does the data go?
 - Is the data retrievable in a standard format?

Summary

- ❑ Select cloud computing services carefully and with your organization's legal requirements and your own information security and privacy policies in mind.
- ❑ Use Common Sense!
- ❑ Consider the cloud computing vendor as much more than just a software provider; it really is another type of business partner.
- ❑ Ask are those silent business partners securing their servers appropriately, and ensuring appropriate privacy protections to the vast amounts of personally identifiable information that is being entrusted to them?

Questions?

Want More Information?

+1 (888) 90-AUDIT / +1 (888) 902-8348
info@controlsolutions.com
www.controlsolutions.com

Allen Lum: alum@controlsolutions.com
Thomas Daggett: tdaggett@controlsolutions.com

ControlSolutions International



www.controlsolutions.com